AN14068

S32K3/S32K1 + FS23 hardware and safety application guide

Rev. 2.0 — 21 November 2024 Application note

Document information

Information	Content
Keywords	FS2300, FS2320, safety, system basis chip (SBC), S32K3, S32K1, Body and Comfort, CAN FD, LIN, ISO 26262, SPI, I²C
Abstract	This application note provides guidelines to attach the FS23 SBC family with S32K3 and S32K1 MCUs into automotive electronic systems.

1 Introduction

This application note provides design guidelines on how to supply NXP's S32K1xx and S32K3xx microcontrollers using NXP's FS23 System Basis Chip family of devices for automotive body systems.

This document discusses system-level details and recommendations when using the dedicated FS23 device to supply NXP S32K1xx/S32K3xx and other peripherals as part of the full system. Using I/Os and built-in functional safety features, the system designer can maximize the safety level up to ASIL B.

This document gives guidance to implement the companionship between FS23 safety basis chips and S32K microcontrollers, with an application diagram and a connection summary for each solution. The document provides information based on typical current values given in S32K microcontroller data sheets. It is left to the discretion of the system designer to verify that the configuration for the application stays within the range of achievable power delivery for FS23 devices.

The document covers the following solutions combining FS23 + S32K:

- FS23 + S32K11x
- FS23 + S32K14x
- FS23 + S32K31x
- FS23 + S32K322
- FS23 + S32K324
- FS23 + S32K341
- FS23 + S32K342
- FS23 + S32K344

Note: *Regarding S32K34x lockstep core MCUs, FS23 devices cover up to ASIL B applications by design. For higher ASIL applications, refer to FS26 devices.*

1.1 General description

The FS23 SBC offers an expandable family of devices that is pin-to-pin and software compatible.

The FS23 SBC is scalable from the linear voltage regulator version to the DC-DC regulator version, as well as from QM to ASIL B.

The FS23 SBC includes CAN and LIN transceivers, along with various system and safety features for the latest generation of automotive electronic control units (ECUs).

The FS23 SBC provides a high-level of integration in order to optimize the bill of material (BOM) cost for the body and comfort market.

Thanks to its flexibility, the FS23 is suitable for S32K processor-based applications, as well as for multi-vendor processors.

Several device versions are available, offering choice of output-voltage settings, operating frequency, power-up sequencing, and inputs/outputs configuration to address multiple applications.

1.2 Features and benefits

1.2.1 Operating modes

- Normal mode with all power management and functional safety features available
- Stop mode: Low-power OFF mode with multiple wake-up sources (LPOFF)
- Standby mode: Low-power ON mode with HVBUCK or HVLDO1 active and multiple wakeup sources (LPON)

1.2.2 Power management

- **HVBUCK:** Synchronous buck converter with integrated FETs. Configurable Normal mode output voltage and LPON mode output voltage (3.3 V or 5.5 V). Output DC current capability of 600 mA in Normal mode, and 100 mA current capability in Low-power ON mode.
- **HVLDO1:** High-voltage LDO instead of the HVBUCK for MCU supply with selectable output voltage (3.3 V or 5.5 V) and up to 100 mA DC current capability with internal PMOS and 250 mA with external PNP.
- **HVLDO2:** High-voltage LDO regulator for system loads, with optional external protection for off-board sensors, selectable output voltage (3.3 V or 5.0 V) and up to 100 mA DC current capability.
- **HVLDO3:** High-voltage LDO regulator for CAN FD block supply or other with selectable output voltage (3.3 V or 5.0 V) and up to 150 mA current capability.

1.2.3 System features

- One CAN FD supporting up to 5 Mbps communication following ISO 11898-2:2016 and SAE J2284 standards
- One LIN following LIN 2.2, ISO 17987-4, and SAE-J2602-2 standards
- Two wake-up inputs (40 V capable)
- Two high-voltage I/Os with wake-up capability (40 V capable)
- Up to four low-voltage I/Os with wake-up capability
- Four configurable high-side drivers with 150 mA drive capability, to supply LEDs or enable external devices (INH), and cyclic sense capability
- Multiple wake-up sources: WAKE pins, HVIO pins, LVIO pins, CAN FD, LIN, or dedicated SPI/I^2C command
- Device control via 32-bit SPI interface or via I^2C interface, with CRC
- Integrated long duration timer (LDT) for system shutdown and wake-up control, programmable duration up to 194 days
- 16-channel analog multiplexer (AMUX) for system monitoring (temperature, battery voltage, internal voltages)

1.2.4 Functional safety

- Developed following ISO 26262:2018 standard to fit for ASIL B applications
- Internal monitoring circuitry with its own reference
- Additional input for external voltage monitoring
- Window or timeout watchdog function to monitor MCU failures by software
- FCCU inputs to monitor MCU failures by hardware
- Analog built-in self-test (ABIST) on demand
- Safety outputs (RSTB, FS0B, LIMP0, and LIMP1/2 with 1.25 Hz or 100 Hz PWM capability)

1.2.5 EMC compliance

- The FS23 EMC tests are performed according to ZVEI Generic IC EMC Test Specification version 2.1 (2017) and FMC1278 Electromagnetic Compatibility Specification for Electrical/Electronic Components and subsystems version 3.0 (2018).

1.2.6 Configuration and enablement

- QFN48EP: QFN 48 pins with exposed pad for optimized thermal management, wettable flanks, 7 mm × 7 mm × 0.85 mm, 0.5 mm pitch, 48 pins
- One time programmable (OTP) memory for scalability, expandability, and device customization
- OTP emulation mode for hardware development and evaluation
- Debug mode for software development, MCU programming, and debugging

1.3 Available documents

Reference documents and various material are available on FS23 device webpage. The webpage provides more detailed information about specific topics:

- FS23 data sheet: Information such as features, functional description, parametric description, register mapping.
- FS23 safety manual (ASIL B): Describes how to use the FS23 in the context of a safety-related system, specifying the user's responsibilities for installation and operation to reach the targeted safety integrity level.
- FS23 Hardware Guidelines application note: Information such as application schematics, bill of materials, and placement and layout guidelines.
- FS23 Implementation and Behavior application note: engineering and operating modes, MCU communication, long duration timer implementation, OTP settings and good practices guidelines.

Reference manuals and hardware design guidelines application notes are also available on S32K1 and S32K3 MCUs' webpages:

- S32K1 Reference Manual and Hardware Design Guidelines: Documents including description of MCU's power system, clock circuitry and interfaces, and general layout guidelines.
- S32K3 Reference Manual: Document covering the power domains and available configurations, pinout description, clock circuitry and interfaces description, and general layout guidelines.

2 Power architecture and device selection

Multiple power architectures are possible, depending on the S32K1 and S32K3 part number and package. This section presents these architectures and provides guidelines to supply S32K1 and S32K3 MCUs using FS23 family of devices.

FS23/S32K part numbering

As a reminder, the part numbering for FS23 and S32K devices is constructed as shown in Figure 1.

For more information on FS23 and S32K part numbering, refer to the FS23, S32K1, and S32K3 data sheets' "Ordering information" sections.

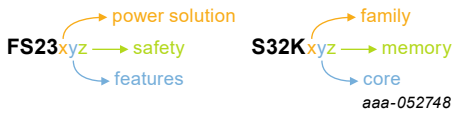

Figure 1. Part numbering

2.1 Single-supply architecture

This power architecture uses one supply rail (5.0 V or 3.3 V) from the FS23 to the MCU supply and reference pins.

MCUs with one main I/O and analog supply voltage

This single-supply architecture is applicable when the MCU has one main I/O and analog supply voltage VDD_HV_A. The compatible references are: S32K1xx devices for all packages, and S32K310 (48LQFP or 100MAXQFP package), S32K311 (48LQFP or 100MAXQFP package), S32K312 (100MAXQFP or 172MAXQFP package), S32K314 (100MAXQFP package).

Figure 2 shows the connections of FS23 as an SBC to compatible S32K1/3 MCUs.

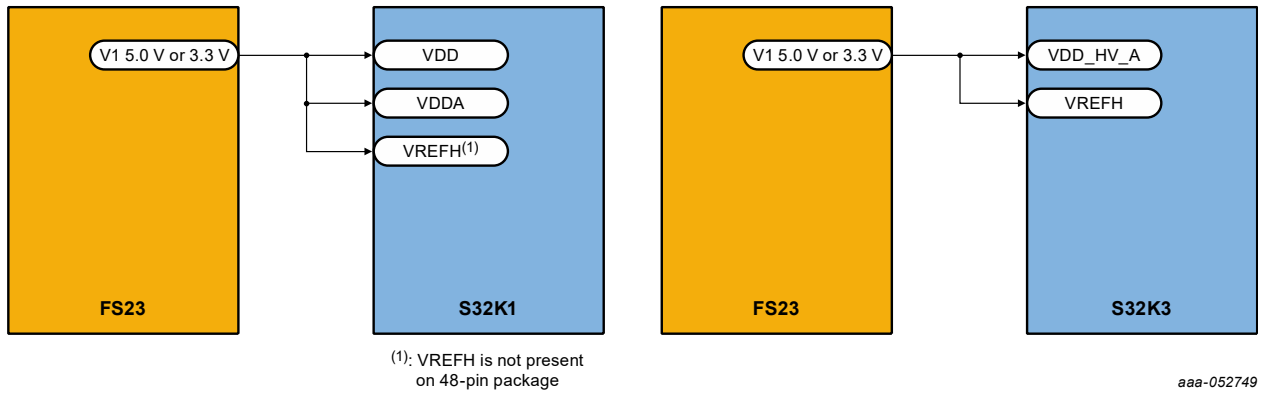

Figure 2. Single-supply architecture

In this case, the 1.1 V high-current core logic supply is internally generated from the 5.0 V or 3.3 V connection to VDD_HV_A pin.

MCUs with secondary I/O supply voltage and high-current logic supply

This single-supply architecture is also applicable to higher performance MCUs with a secondary I/O supply voltage VDD_HV_B and a high-current logic supply V15. In this case, it requires an external NPN transistor to supply 1.5 V high-current logic.

The compatible references are: S32K314 (172MAXQFP or 257MBGA package), S32K322 (100MAXQFP or 172MAXQFP package), S32K324 (172MAXQFP or 257MBGA package), S32K341 (100MAXQFP or 172MAXQFP package), S32K342 (100MAXQFP or 172MAXQFP package), and S32K344 (172MAXQFP or 257MBGA package).

Figure 3 shows the connections of FS23 as an SBC to compatible MCUs.

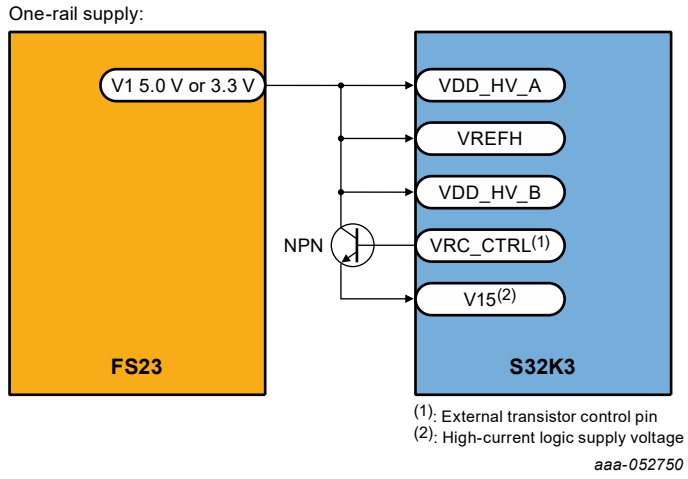

Figure 3. Single-supply architecture with external transistor for V15

In this case, the 1.1 V high-current core logic supply is internally generated from the V15 pin connection. The external NPN transistor's VC_BJT pin can either be connected to VDD_HV_A or VDD_HV_B (3.3 V or 5.0 V). More information on supplying V15 from the NPN transistor option is available in section "Using a BJT for 1.5 V generation" of the S32K3 Reference Manual document.

2.2 Dual-supply architecture

A dual supply architecture is applicable to higher performance MCUs with a secondary I/O supply voltage VDD_HV_B and a high-current logic supply V15. In this case, it requires an external NPN transistor to supply 1.5 V high-current logic.

The compatible references are: S32K314 (172MAXQFP or 257MBGA package), S32K322 (100MAXQFP or 172MAXQFP package), S32K324 (172MAXQFP or 257MBGA package), S32K341 (100MAXQFP or 172MAXQFP package), S32K342 (100MAXQFP or 172MAXQFP package), and S32K344 (172MAXQFP or 257MBGA package).

Figure 4 shows the connections of FS23 as a system basis-chip to compatible MCUs.

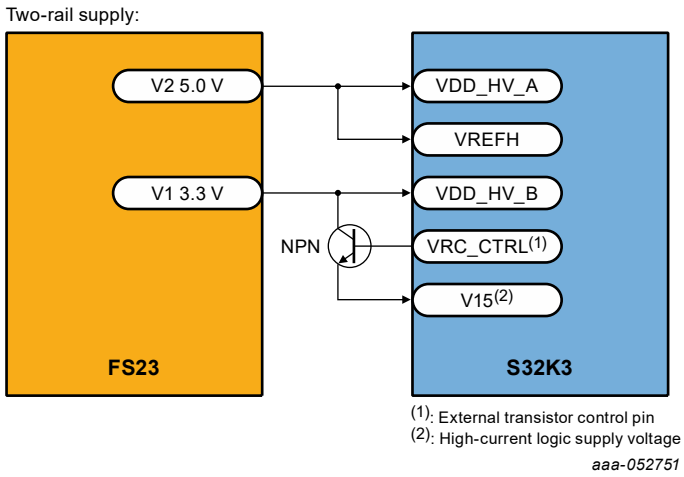

Figure 4. Dual-supply architecture with external transistor for V15

In this case, the 1.1 V high-current core logic supply is internally generated from the V15 pin connection. The external NPN transistor's VC_BJT pin can either be connected to VDD_HV_A or VDD_HV_B (3.3V or 5.0V). More information on supplying V15 from the NPN transistor option is available in section "Using a BJT for 1.5 V generation" of the S32K3 reference manual document.

2.3 FS23 vs. S32K1/S32K3 mapping

This section suggests a mapping of the FS23 SBC family and the S32K1/S32K3 MCU series, based only on the MCU supply requirements. Depending on the system aspects (the integrated physical layers, the features, the safety-level target, and so on) more appropriate solutions can be found. FS23 devices are QM and ASIL B compatible. An optimized FS23 version is proposed for each MCU sub-family (in green). It is assumed that higher-end FS23 versions can also address this MCU sub-family.

Table 1 shows the mapping of FS23 devices vs. S32K1/3 devices based on the MCU supply requirements. On the X-axis, S32K1/3 devices listed in order of maximum current consumption. On the Y-axis, FS23 devices with the main regulator's (V1) maximum current capability.

Table 1. FS23 vs. S32K1/S32K3 mapping

FS23 ($I_{max,V1}$)	**S32K1 family**			**S32K3 family**		
	S32K116 S32K118	S32K14xW	S32K142 S32K144 S32K146 S32K148	S32K310 S32K311 S32K312	S32K314 S32K322 S32K324	S32K341 S32K342 S32K344
FS230xy (100 mA)	✓	✓				
FS230xy + ext. PNP (250 mA)	✓	✓	✓	✓		
FS232xy (600 mA)	✓	✓	✓	✓	✓	✓

3 Hardware implementation

This section describes the hardware implementation of FS23 and S32K1 or S32K3 safety features.

It also provides bill of material and layout recommendations.

3.1 Safety pins connections between FS23 and S32K1xx/S32K3xx

As both the FS23 and S32K1/3 devices have many pins, this section highlights specifically the safety-related SBC and MCU pins.

The terminals described in this section are safety related and must be connected to enhance the full functional safety features of the S32K1/3 and FS23 devices. Table 2 and Table 3 below list all safety-related pin connections between the FS23 and S32K1/3.

Table 2. FS23 and S32K1 safety pins connections

FS23 pin name	FS23 pin description	Connect with	S32K1 pin description	S32K1 pin name
V1	V1 regulator output voltage	⇔	Main voltage supply	VDD
V1	V1 regulator output voltage	⇔	Analog voltage supply	VDDA
V1	V1 regulator output voltage (±2% accuracy)	⇔	ADC high-voltage reference supply	VREFH
PGND, GND_IO	Ground connections	⇔	Supply ground	VSS
RSTB	Reset Input / Output	⇔	Reset Input / Output	RESET_b
FCCU1	Fault Collection and Control Unit 1	⇔[1]	I/O port	PTxn
FCCU2[2]	Fault Collection and Control Unit 2	⇔[1]	I/O port	PTxn

[1] S32K1 family does not provide a fault collection and control unit. Nonetheless, FCCUx pins on FS23 can still be used as monitoring inputs, depending on system-safety requirements. FCCUx input pins on FS23 can be configured to monitor a level or a PWM. They are configured during INIT configuration.

[2] FCCU2 is not visible on FS23 pinout. FCCU2 must be configured during INIT phase as a function on any input among HVIO1, HVIO2, LVIO3, LVIO4 and LVI5 via FCCU2_ASSIGN[2:0] bits.

Table 3. FS23 and S32K3 safety pins connections

FS23 pin name	FS23 pin description	Connect with	S32K3 pin description	S32K3 pin name
V1 or V2[1]	V1 or V2 regulator output voltage	⇔	Main I/O voltage supply	VDD_HV_A
V1 or V2[1]	V1 or V2 regulator output voltage (±2 % accuracy)	⇔	ADC high-voltage reference supply	VREFH
V1	*V1 regulator output voltage*	⇔[2]	*Other I/O domain voltage supply*	*VDD_HV_B*
V1	*V1 regulator output voltage (±2 % accuracy)*	⇐NPN⇒[3]	*1.5 V high-current logic supply*	*V15*
PGND, GND_IO	Ground connections	⇔	Core logic ground supply	VSS
RSTB	Reset input/output	⇔	Reset input/output	RESET_b
FCCU1	Fault collection and control unit 1	⇔	FCCU error 0 output	FCCU_ERR0
FCCU2[4]	Fault collection and control unit 2	⇔	FCCU error 1 output	FCCU_ERR1

[1] Depends on chosen FS23 + S32K3 power supply architecture.
[2] Depends on S32K3 part number.
[3] Depends on S32K3 part number, connected though an external NPN transistor.
[4] FCCU2 is not visible on FS23 pinout. FCCU2 must be configured during INIT phase as a function on any input among HVIO1, HVIO2, LVIO3, LVIO4 and LVI5 via FCCU2_ASSIGN[2:0] bits. FCCU monitoring necessarily follows the bi-stable protocol when S32K3 is used. FCCUx input pins on FS23 are configured during INIT configuration.

Table 4. FS23 and S32K1/3 communication pins connections

FS23 pin name	FS23 pin description	Connect with[1]	MCU communication pin description	MCU communication pin name
SCK	SPI clock input	⇔	LPSPI serial clock I/O	LPSPIx_SCK
MOSI	SPI master out slave input	⇔	LPSPI serial data output	LPSPIx_SOUT
MISO	SPI master input slave out	⇔	LPSPI serial data input	LPSPIx_SIN
CSB	SPI chip select	⇔	Peripheral chip select	LPSPIx_PCS[0]
SCL	I²C clock input	⇔	LPI2C serial clock line	LPI2Cx_SCL
SDA	I²C bidirectional data line	⇔	LPI2C serial data line	LPI2Cx_SDA

[1] Depends on chosen communication bus.

3.2 Single-supply architecture

Figure 5 shows the hardware connections to implement the one-rail power architecture with an FS230x (V1 is HVLDO1) and an MCU from S32K1 family.

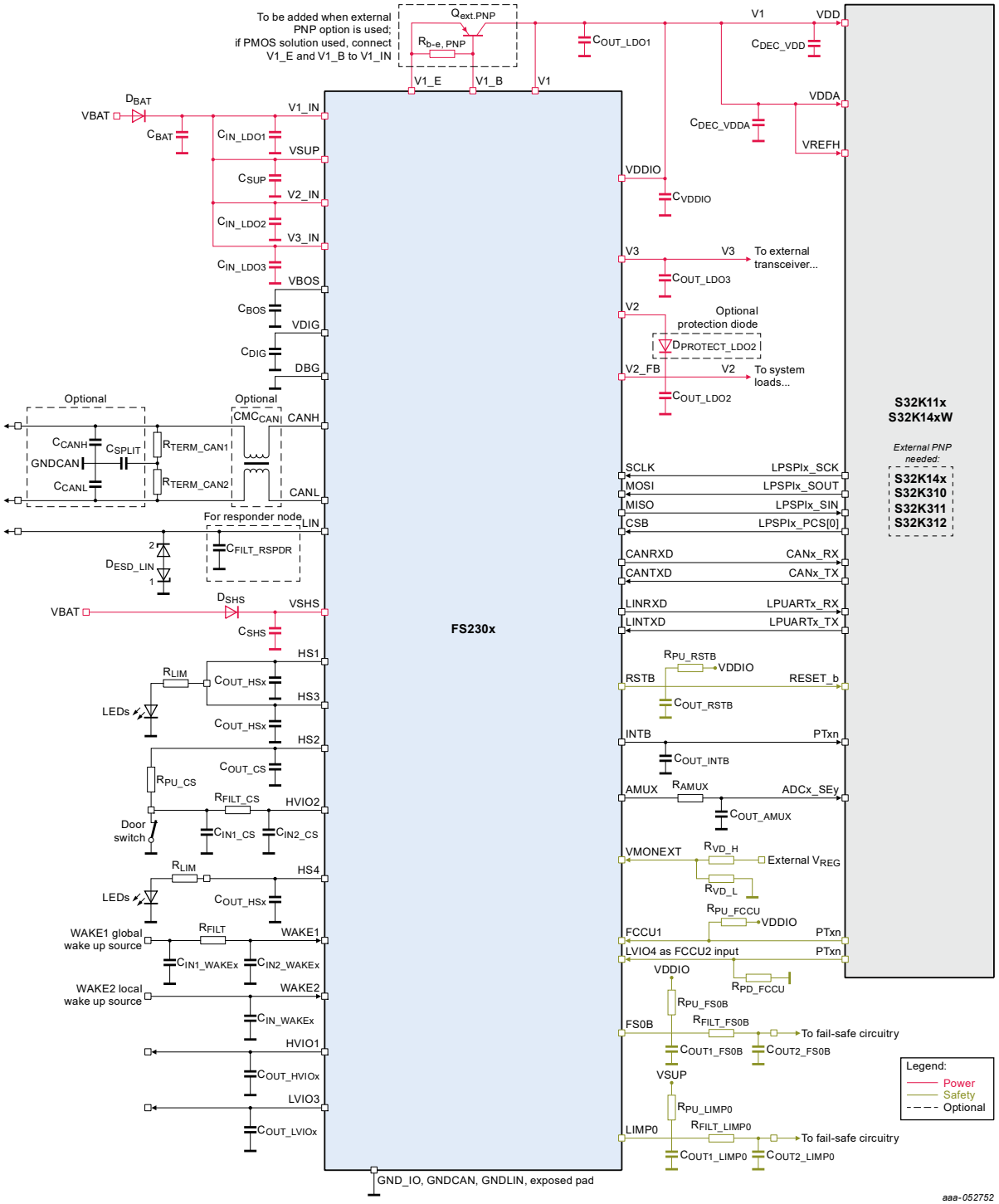

Figure 5. One-rail power supply architecture with FS230x

Figure 6 shows the hardware connections to implement the one-rail power architecture with an FS232x (V1 is HVBUCK) and compatible S32K3 devices.

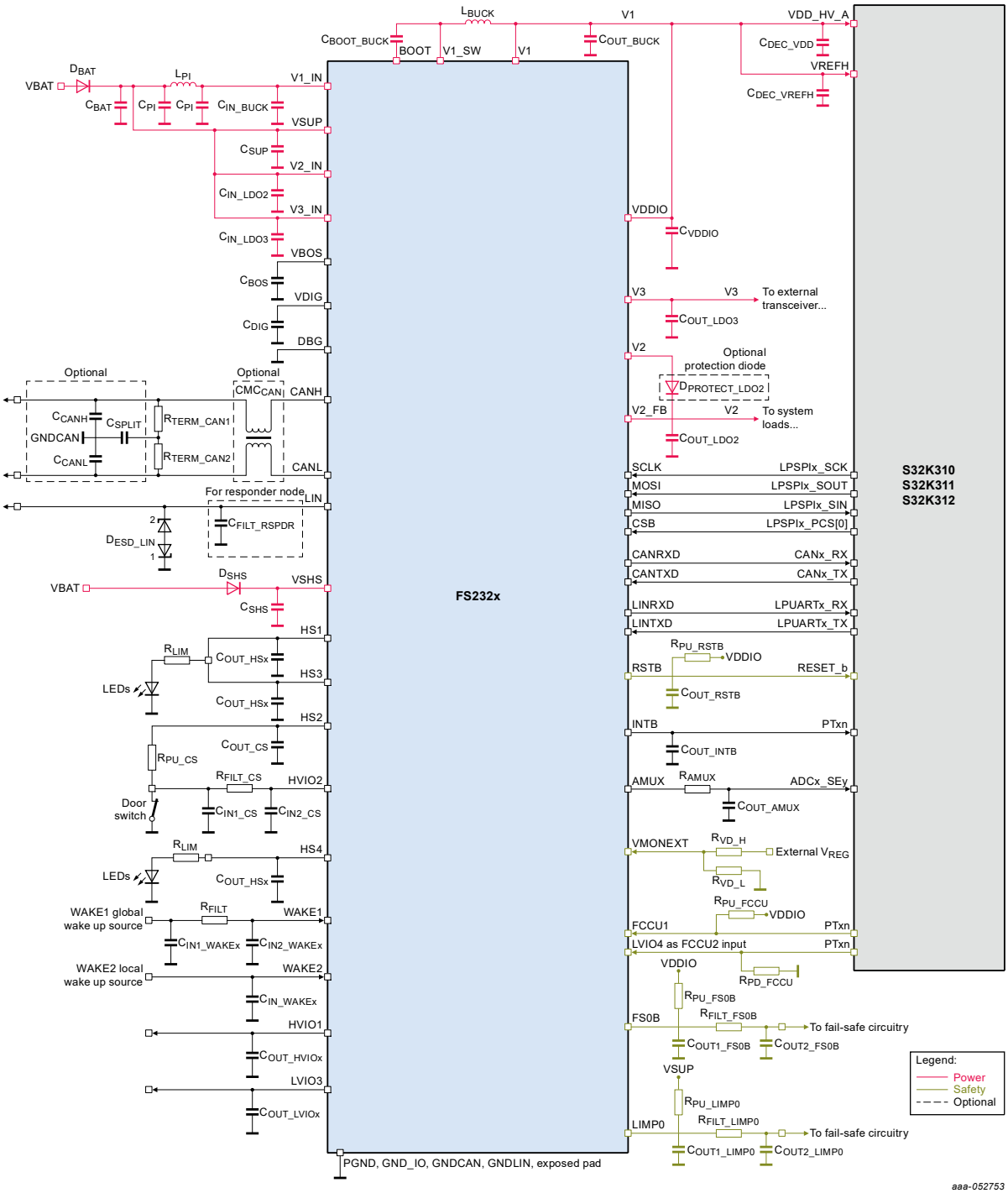

Figure 6. One-rail power supply architecture with FS232x

3.3 Single-supply with external NPN for V15 architecture

Figure 7 shows the hardware connections to implement the one-rail power architecture with external NPN transistor for an FS232x (V1 is HVBUCK) and compatible S32K3 devices.

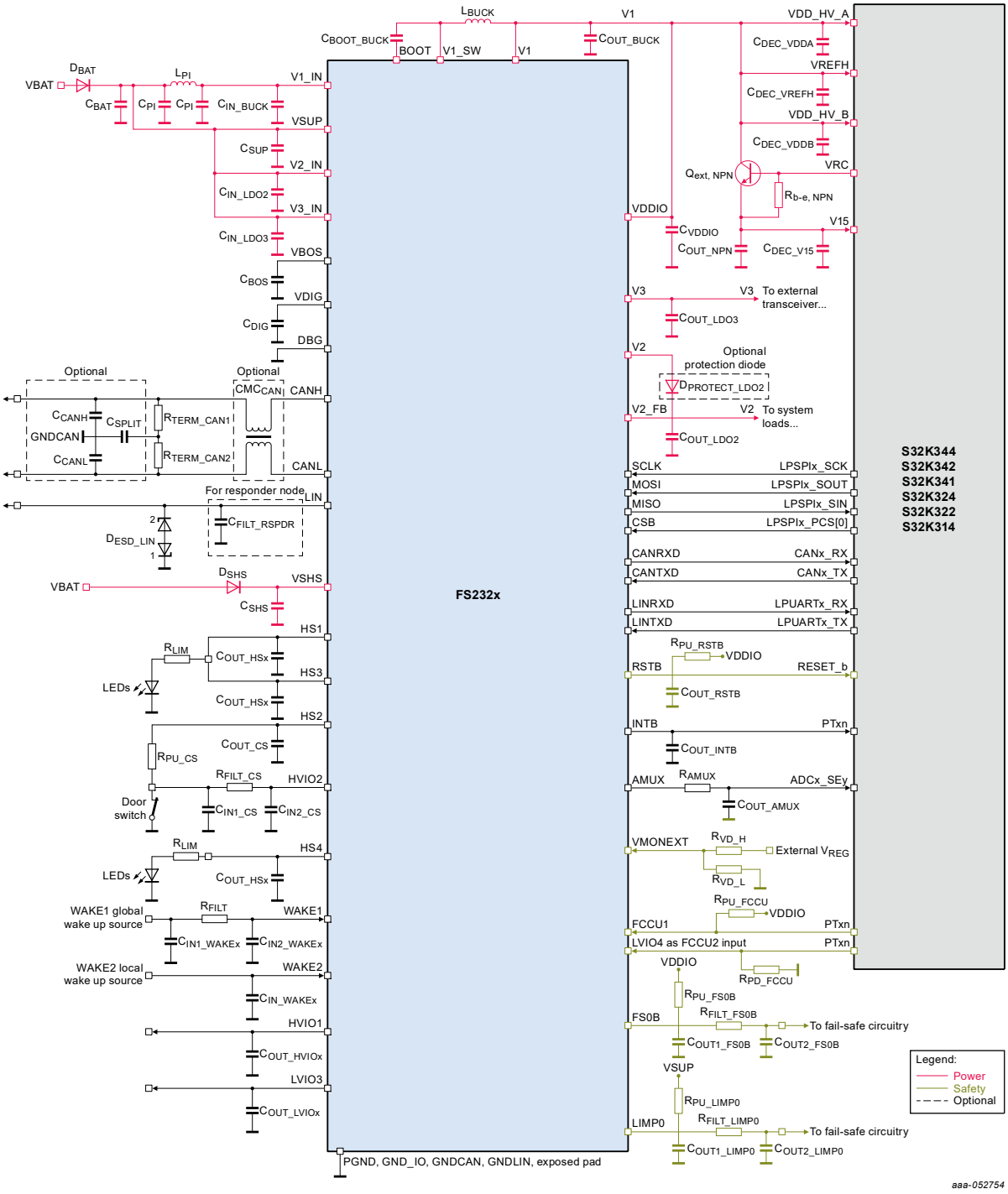

Figure 7. One-rail power supply architecture with external transistor

3.4 Dual-supply with external NPN for V15 architecture

Figure 8 shows the hardware connections to implement the two-rail power architecture with external NPN transistor for an FS232x (V1 is HVBUCK) and compatible S32K3 devices.

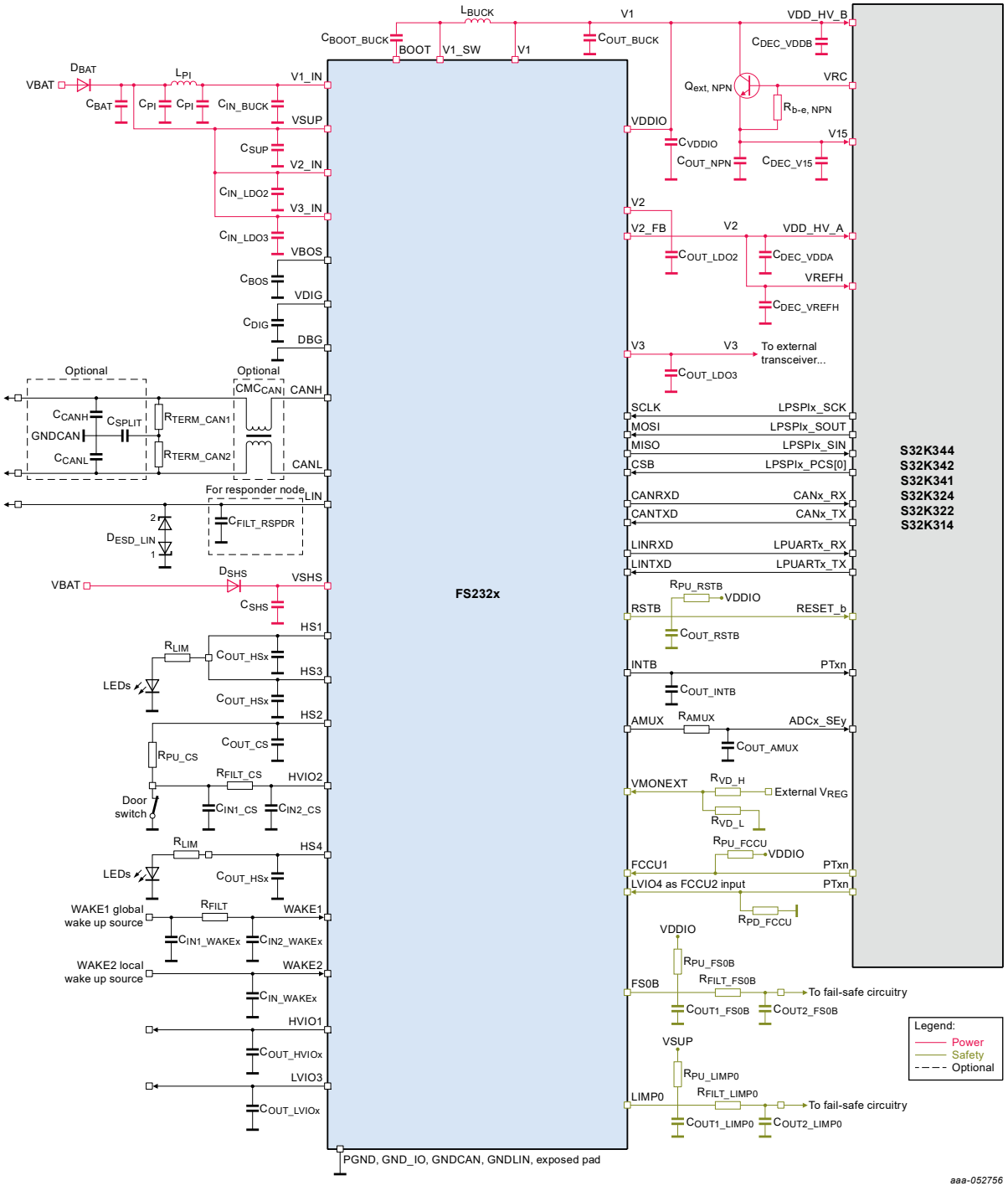

Figure 8. Two-rail power supply architecture with external transistor

3.5 Bill of materials

The general bill of materials below is given as a reference. Components are listed in alphabetical order to facilitate readability simultaneously with the applications schematics provided above.

More information about component choice is available in the FS23 hardware guidelines application note and S32K1 and S32K3 documentation (see Section 6).

Designator	Value	Description	Vendor	Part number	Comment
C_{BAT}	2 x 10 µF	CAP CER 10 uF 50 V 10 % X7S AEC-Q200 1210	TDK	CGA6P3X7S1H106K250AE	Soft termination Could be replaced by a 22 nF capacitor
	+ 100 nF	CAP CER 0.1 uF 50 V 10 % X7R AEC-Q200 0603	TDK	CGA3E2X7R1H104K080AA	Optional
C_{BOOT_BUCK}	33 nF	CAP CER 0.033 uF 50 V 10 % X7R AEC-Q200 0603	TDK	CGA3E2X7R1H333K080AA	
C_{BOS}	1 µF	CAP CER 1 uF 16 V 10 % X7R AEC-Q200 0603	TDK	CGA3E1X7R1C105K080AC	
C_{DIG}	1 µF	CAP CER 1 uF 16 V 10 % X7R AEC-Q200 0603	TDK	CGA3E1X7R1C105K080AC	
C_{DEC_V15}	Refer to S32K1 and S32K3 documentation (see Section 1.3).				
C_{DEC_VDD}	Refer to S32K1 and S32K3 documentation (see Section 1.3).				
C_{DEC_VDDA}	Refer to S32K1 and S32K3 documentation (see Section 1.3).				
C_{DEC_VDDB}	Refer to S32K1 and S32K3 documentation (see Section 1.3).				
C_{DEC_VREFH}	Refer to S32K1 and S32K3 documentation (see Section 1.3).				
C_{CANH}, C_{CANL}	100 pF	CAP CER 100 pF 100 V 5 % C0G AEC-Q200 0603	MURATA	GCM1885C2A101JA16D	
C_{IN_BUCK}	10 µF	CAP CER 10 uF 50 V 10 % X7S AEC-Q200 1210	TDK	CGA6P3X7S1H106K250AE	When f_{SW} is 450 MHz
	4.7 µF	CAP CER 4.7 uF 50 V 10 % X7R AEC-Q200 1210	MURATA	GCJ32ER71H475KA12L	When f_{SW} is 2.2 MHz
C_{IN_LDO1}	1.0 µF	CAP CER 1.0 uF 50 V 10 % X7R AEC-Q200 0805	TDK	CGA4J3X7R1H105K125AB	
C_{IN_LDO2}	1.0 µF	CAP CER 1.0 uF 50 V 10 % X7R AEC-Q200 0805	TDK	CGA4J3X7R1H105K125AB	
C_{IN_LDO3}	1.0 µF	CAP CER 1.0 uF 50 V 10 % X7R AEC-Q200 0805	TDK	CGA4J3X7R1H105K125AB	
C_{IN_WAKEx}	10 nF	CAP CER 0.01 uF 50 V 10 % X7R AEC-Q200 0603	TDK	CGA3E2X7R1H103K080AA	
C_{IN1_CS}	10 nF	CAP CER 0.01 uF 50 V 10 % X7R AEC-Q200 0603	TDK	CGA3E2X7R1H103K080AA	
C_{IN2_CS}	1 nF	CAP CER 1000 pF 50 V 5 % C0G AEC-Q200 0603	TDK	CGA3E2C0G1H102J080AA	10 nF is recommended in case ISO pulses are applicable.
C_{IN1_WAKEx}	22 nF	CAP CER 0.022 uF 50 V 10 % X7R AEC-Q200 0603	TDK	CGA3E2X7R1H223K080AA	
C_{IN2_WAKEx}	10 nF	CAP CER 0.01 uF 50 V 10 % X7R AEC-Q200 0603	TDK	CGA3E2X7R1H103K080AA	
C_{OUT_AMUX}	1 nF	CAP CER 1000 pF 50 V 5 % C0G AEC-Q200 0603	TDK	CGA3E2C0G1H102J080AA	

Designator	Value	Description	Vendor	Part number	Comment
C_{OUT_BUCK}	4 x 10 µF	CAP CER 10 uF 16 V 10 % X7S AEC-Q200 0805	TDK	CGA4J1X7S1C106K125AC	When f_{SW} is 450 kHz (V_{OUT} = 5.0 V)
	5 x 10 µF	CAP CER 10 uF 16 V 10 % X7S AEC-Q200 0805	TDK	CGA4J1X7S1C106K125AC	When f_{SW} is 450 kHz (V_{OUT} = 3.3 V)
	10 µF	CAP CER 10 uF 16 V 10 % X7S AEC-Q200 0805	TDK	CGA4J1X7S1C106K125AC	When f_{SW} is 2.2 MHz (V_{OUT} = 5.0 V)
	2 x 10 µF	CAP CER 10 uF 16 V 10 % X7S AEC-Q200 0805	TDK	CGA4J1X7S1C106K125AC	When f_{SW} is 2.2 MHz (V_{OUT} = 3.3 V)
	+ 100 nF	CAP CER 0.1 uF 16 V 10 % X7R AEC-Q200 0402	MURATA	GCM155R71C104KA55D	Optional
C_{OUT_CS}	1 nF	CAP CER 1000 pF 50 V 5 % C0G AEC-Q200 0603	TDK	CGA3E2C0G1H102J080AA	Optional
C_{OUT_INTB}	1 nF	CAP CER 1000 pF 50 V 5 % C0G AEC-Q200 0603	TDK	CGA3E2C0G1H102J080AA	
C_{OUT_LVIOx}	10 nF	CAP CER 0.01 uF 50 V 10 % X7R AEC-Q200 0603	TDK	CGA3E2X7R1H103K080AA	
C_{OUT_HSx}	33 nF	CAP CER 0.033 uF 50 V 10 % X7R AEC-Q200 0603	SAMSUNG	CL10B333KB85PNC	
	+ 47 pF	CAP CER 47 pF 50 V 5 % C0G AEC-Q200 0603	TDK	CGA3E2C0G1H470J080AA	
C_{OUT_HVIOx}	10 nF	CAP CER 0.01 uF 50 V 10 % X7R AEC-Q200 0603	TDK	CGA3E2X7R1H103K080AA	
C_{OUT_LDO1}	2.2 µF	CAP CER 2.2 uF 16 V 10 % X7R AEC-Q200 0805	TDK	CGA4J3X7R1C225K125AB	Without external PNP
	10 µF	CAP CER 10 uF 16 V 10 % X7S AEC-Q200 0805	TDK	CGA4J1X7S1C106K125AC	With external PNP
C_{OUT_LDO2}	2.2 µF	CAP CER 2.2 uF 16 V 10 % X7R AEC-Q200 0805	TDK	CGA4J3X7R1C225K125AB	
	+ 100nF	CAP CER 0.1 uF 16 V 10 % X7R AEC-Q200 0402	MURATA	GCM155R71C104KA55D	Optional
C_{OUT_LDO3}	2.2 µF	CAP CER 2.2 uF 16 V 10 % X7R AEC-Q200 0805	TDK	CGA4J3X7R1C225K125AB	
	+ 100nF	CAP CER 0.1 uF 16 V 10 % X7R AEC-Q200 0402	MURATA	GCM155R71C104KA55D	Optional
C_{OUT_NPN}	Refer to S32K1 and S32K3 documentation (see Section 1.3).				
C_{OUT_RSTB}	1 nF	CAP CER 1000 pF 50 V 5 % C0G AEC-Q200 0603	TDK	CGA3E2C0G1H102J080AA	
C_{OUT1_LIMP0}	10 nF	CAP CER 0.01 uF 50 V 10 % X7R AEC-Q200 0603	TDK	CGA3E2X7R1H103K080AA	
C_{OUT2_LIMP0}	22 nF	CAP CER 0.022 uF 50 V 10 % X7R AEC-Q200 0603	TDK	CGA3E2X7R1H223K080AA	
C_{OUT1_FS0B}	10 nF	CAP CER 0.01 uF 50 V 10 % X7R AEC-Q200 0603	TDK	CGA3E2X7R1H103K080AA	
C_{OUT2_FS0B}	22 nF	CAP CER 0.022 uF 50 V 10 % X7R AEC-Q200 0603	TDK	CGA3E2X7R1H223K080AA	
C_{PI}	10 µF	CAP CER 10 uF 50 V 10 % X7S AEC-Q200 1210	TDK	CGA6P3X7S1H106K250AE	
C_{SHS}	10 µF	CAP CER 10 uF 50 V 10 % X7S AEC-Q200 1210	TDK	CGA6P3X7S1H106K250AE	
C_{SPLIT}	4.7 nF	CAP CER 4700 pF 50 V 5 % C0G AEC-Q200 0603	KEMET	C0603C472J5GACAUTO	
C_{SUP}	1 nF	CAP CER 1000 pF 50 V 5 % C0G AEC-Q200 0603	TDK	CGA3E2C0G1H102J080AA	Optional
C_{VDDIO}	100 nF	CAP CER 0.1 uF 16 V 10 % X7R AEC-Q200 0402	MURATA	GCM155R71C104KA55D	

Designator	Value	Description	Vendor	Part number	Comment
CMC_{CAN}	100u H@100KHZ	FILTER COMMON MODE 100 uH@100 KHZ 150mA +50/-30 % AEC-Q200 SMT	TDK	ACT1210-101-2P-TL00	Optional depending on CAN EMC requirements.
D_{BAT}	N/A	DIODE SCH RECT 2 A 40 V AEC-Q101 SOD123W	NEXPERIA	PMEG4020ER-QX	Reverse battery protection diode
D_{ESD_LIN}	N/A	ESD Suppressor AEC-Q101	NEXPERIA	PESD1IVN27	
$D_{PROTECT\_LDO2}$	N/A	DIODE SCH 0.5 A 40 V AEC-Q101 SOD323F	NEXPERIA	PMEG4005EJ-QF	Optional protection diode against short to battery.
D_{SHS}	N/A	DIODE SCH RECT 2 A 40 V AEC-Q101 SOD123W	NEXPERIA	PMEG4020ER-QX	Reverse battery protection diode
L_{BUCK}	22 µH	IND PWR 22 uH@100 kHz 1.42 A 20 % AEC-Q200 / IND FER 22 uH @ 1 MHz 0.45 A 20 % AEC-Q200	TDK	CLF5030NIT-220M-D / VLS3015CX-220M-H	When f_{SW} is 450 kHz: CLF5030NIT-220M-D (max. 1.1 A) or VLS3015CX-220M-H (max. 450 mA)
	4.7 µH	IND FER 4.7 uH@1 MHz 1.7A 0.12 OHM 20 % AEC-Q200 / IND PWR 4.7 uH@1 MHz 2.2A 20 % AEC-Q200	TDK	VLS3015CX-4R7M-H / TFM252012ALMA4R7MTAA	When f_{SW} is 2.2 MHz
L_{PI}	1 µH	IND WW 1 uH @ 7.96 MHz 1.7 A 20 % AEC-Q200 1210	TDK	NLCV32T-1R0M-EFRD	
$Q_{ext.NPN}$	Refer to S32K1 and S32K3 documentation (see Section 1.3).				
$Q_{ext.PNP}$	N/A	TRAN PNP 1 A 80 V SOT223	NEXPERIA	BCP53-16,115	
R_{AMUX}	200 Ω	RES MF 200 OHM 1/8 W 5 % AEC-Q200 0603	KOA SPEER	RK73B1JTTD201J	
$R_{b\text{-}e,PNP}$	100 kΩ	Thick Film Resistors - SMD 0.2 W 100 Kohms 1 % High Power AEC-Q200	VISHAY	CRCW0402100KFKEDHP	Optional
$R_{b\text{-}e,NPN}$	Refer to S32K1 and S32K3 documentation (see Section 1.3).				
R_{FILT}	5.1 kΩ	RES MF 5.1 K OHM 1/8 W 5 % 0805	PANASONIC	ERJ-6GEYJ512V	Minimum size is 0805
R_{FILT_CS}	10 kΩ	RES MF 10 K 1/8 W 1 % AEC-Q200 0805	VISHAY	CRCW080510K0FKEA	Minimum size is 0805
R_{FILT_FS0B}	5.1 kΩ	RES MF 5.1 K OHM 1/8 W 5 % 0805	PANASONIC	ERJ-6GEYJ512V	Minimum size is 0805
R_{FILT_LIMP0}	5.1 kΩ	RES MF 5.1 K OHM 1/8W 5 % 0805	PANASONIC	ERJ-6GEYJ512V	Minimum size is 0805
R_{PD_FCCU}	22 kΩ	RES MF 22 K 1/10 W 1 % AEC-Q200 0402	KOA SPEER	RK73H1ETTP2202F	
R_{PU_CS}	10 kΩ	RES MF 10 K 1/8 W 1 % AEC-Q200 0805	VISHAY	CRCW080510K0FKEA	
R_{PU_FCCU}	5.1 kΩ	RES MF 5.1 K 1/10W 5 % 0603	VISHAY	CRCW06035K10JNEA	
R_{PU_FS0B}	5.1 kΩ	RES MF 5.1 K 1/10W 5 % 0603	VISHAY	CRCW06035K10JNEA	
R_{PU_LIMP0}	5.1 kΩ	RES MF 5.1 K 1/10W 5 % 0603	VISHAY	CRCW06035K10JNEA	When pulled up to V_{DDIO}
	10 kΩ	RES MF 10 K 1/10 W 0.05 % AEC-Q200 0603	SUSUMU	RG1608N-103-W-T1	When pulled up to V_{SUP}
R_{PU_RSTB}	5.1 kΩ	RES MF 5.1 K 1/10 W 5 % 0603	VISHAY	CRCW06035K10JNEA	
R_{TERM_CANx}	60 Ω	RES MF 60.4 OHM 1/10 W 1 % AEC-Q200 0603	VISHAY	CRCW060360R4FKEA	Two 60 Ω resistors if C_{SPLIT} is used, or simple 120 Ω resistor if C_{SPLIT} unused
R_{VD_H}	11.7 kΩ	RES 11.7 K 1/16 W 1 % AEC-Q200 0402	KOA SPEER	RN73H1ETTP1172F25	Example values for external V_{REG} = 3.3 V
R_{VD_L}	5.1 kΩ	RES MF 5.1 K 1/10 W 1 % AEC-Q200 0402	KOA SPEER	RK73H1ETTP5101F	$V_{MON\_INPUT} * R_{VD\_L} / (R_{VD\_L} + R_{VD\_H})$ = 1.0 V

3.6 Layout recommendations

The FS23 package is a QFN 48-pin package with exposed pad for enhanced thermal dissipation. Details of the PCB footprint design are available in the Package Drawing section of the FS23 data sheet.

When using four PCB layers, the recommended distribution is the following:

- L1: Top layer used as DC-DC power plane
- L2: System ground
- L3: Power island/signal
- L4: System ground

3.6.1 Example of component placement

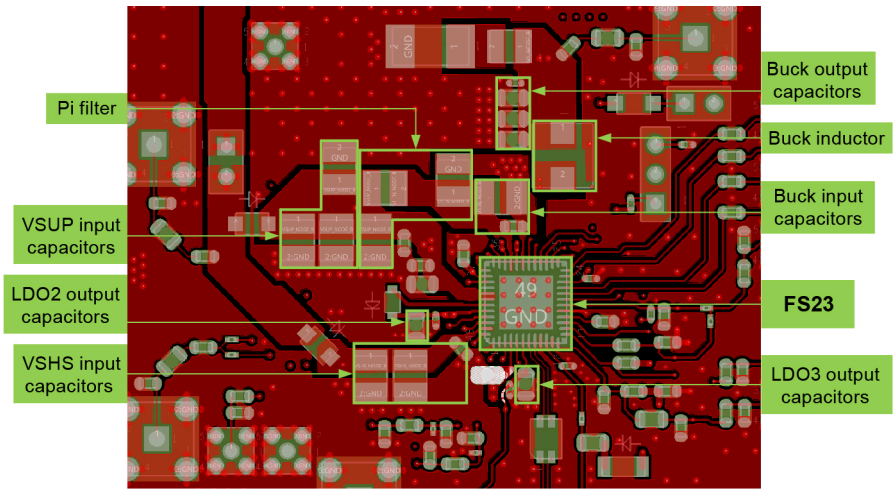

Figure 9. Example of component placement – Top PCB view (V1 is HVBUCK @ 450 kHz)

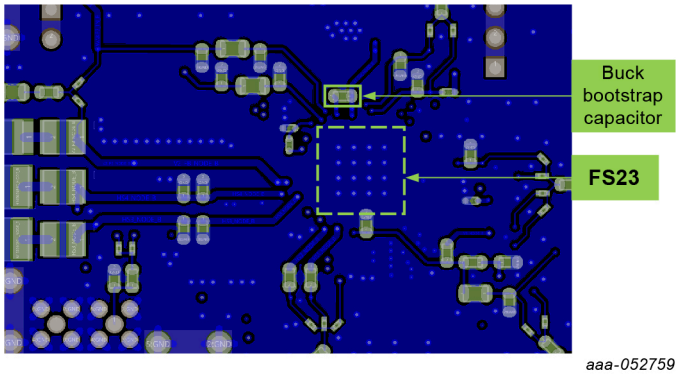

Figure 10. Example of component placement – Bottom PCB view (V1 is HVBUCK @ 450 kHz)

3.6.2 General recommendations

- If a high-current loop is going through multiple PCB layers, multiple vias are recommended to limit the parasitic resistance and inductance (R and L) in the high-current path.
- When a signal is going through multiple PCB layers, ground vias around the layer interconnection are recommended to contain the electrical field.
- Route feedback and control of regulators as short as possible, and shield by ground.
- Separate sensitive and switching signals by ground planes and avoid overlap.
- To avoid noise injection, connect components with high-impedance signals close to the device pin.
- When crossing a sensitive signal with a power trace, have them crossing orthogonally to avoid coupling.
- Connect FS23 exposed pad to ground.
- Place as many vias as possible below the FS23 exposed pad (4x4 grid minimum).
- Do not connect the exposed pad directly to the product GND pins.

3.6.3 HVBUCK specific recommendations

- Avoid low-level signals below HVBUCK components.
- To optimize regulation loop performances, reduce HVBUCK current loop as much as possible with wide tracks:
  - Connect HVBUCK input capacitor as close as possible to V1_IN pin, and position it to allow direct connection between PGND pin and the capacitor ground.
  - The ground of HVBUCK input and output capacitors should be connected close together to minimize ground shift.
- Do not connect PGND ground shape directly to the ground of top layer to avoid any coupling of the noise to the battery. Connect PGND through vias to an underlying layer.
- Place the HVBUCK input pi filter close to the V1_IN pin.
- Place the HVBUCK bootstrap capacitor as close as possible to the FS23 pin. In the example of component placement, the bootstrap capacitor is placed on the bottom layer.
- Connect the HVBUCK feedback close to its load and output capacitors.
- Shield the HVBUCK feedback line (connected to V1 pin) by surrounding the trace with GND.

3.6.4 Pi filter specific recommendations

- Do not route HVBUCK or LDO traces close to the pi filter and VSUP or VSHS connections.
- Connect the pi filter input and output capacitors on different GND polygons.
- Connect the pi filter input capacitor to the same GND as VSUP input capacitors.

3.6.5 Communication buses specific recommendations

- Place ground between I²C SDA and SCL signals, or SPI CSB, SCL, MOSI, and MISO signals.
- Route CANH and CANL as a pair with 120 Ω impedance. Keep the routing symmetrical.
- Shield CANH, CANL, and LIN signals.
- Separate CAN GND from LIN GND.

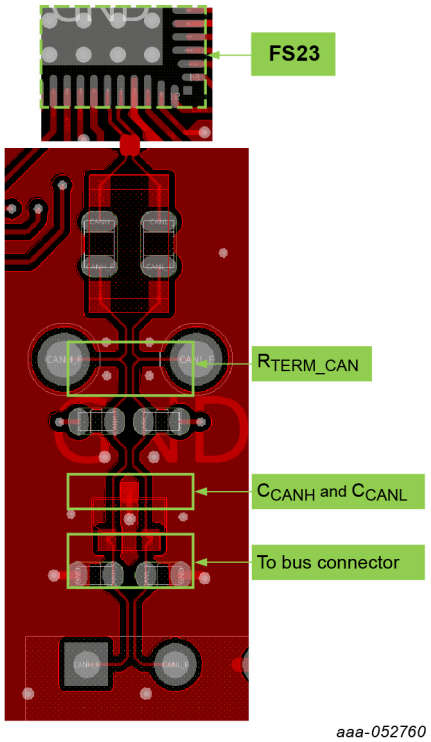

Figure 11. Example of component placement - CAN bus as a pair

4 Software implementation of safety features

4.1 Operation modes

The S32K1/S32K3 family safety concept is a system solution developed to ensure that the platform on which the application is running is protected against random hardware failures, as well as common mode failures.

The safety concept solution relies on S32K1/S32K3 on-chip safety functions and an interface to the safety functions on an external device, in this case the Safety SBC FS23.

The FS23 SBC provides off-chip safety mechanisms, which can move the system to a safe state when the MCU is no longer functioning correctly. The FS23 also monitors its own functions and moves the system to a safe state when an internal failure occurs.

The following sub-sections provide an overview of the interactions between the MCU and the FS23 during the various modes of operation that ensure safe execution of the safety function(s).

4.1.1 Start and boot

First, the FS23 starts up following the pre-configured sequence, then S32K1 or S32K3 starts up and undergoes an internal state transition until both the SBC and the MCU subsequently enter Boot mode. ABIST on demand can be run once the FS23 has entered Normal mode. The boot is a particular mode in which the initialization (INIT) configuration is entered, and watchdog and FCCU can be disabled. For a more detailed sequence, refer to the "Power Management" section of the S32K1 and S32K3 reference manuals.

4.1.1.1 Startup sequence

Start mode begins with the FS23 internal supply reaching regulation and the default OTP configuration being loaded. The system then switches on the output regulators based on the respective OTP configuration of the device. At this moment, the MCU starts up and undergoes an internal state transition. Once both the SBC and the MCU complete startup, Boot mode is entered.

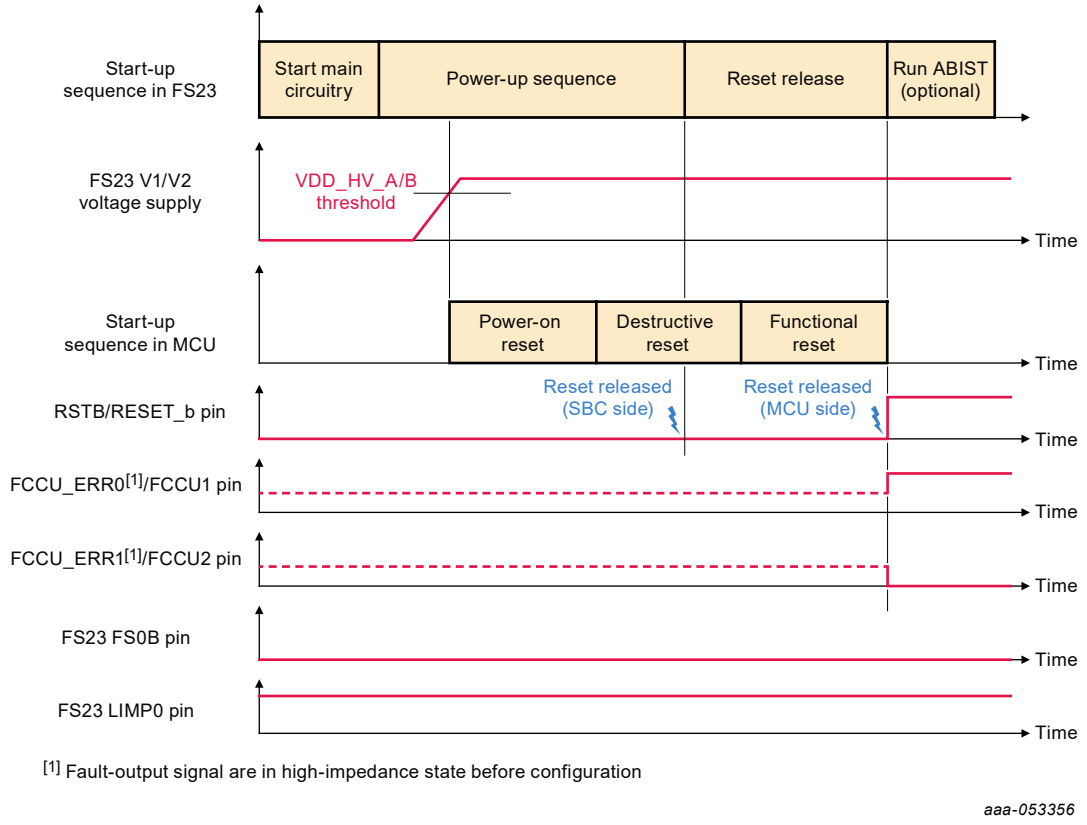

Figure 12. Startup sequence

4.1.1.2 ABIST on demand

The ABIST included in the FS23 checks all the voltage comparators that are used to detect under- and overvoltage faults. The ABIST is executed on demand, after an SPI or I^2C request from the MCU.

On the FS23, the ABIST is not executed automatically at startup. It can be launched from Normal mode only. It is recommended to run ABIST after the power-up sequence to verify the correct functionality of the safety analog circuits. The status bit ABIST_READY notifies that ABIST is available and ready to be launched.

ABIST can be launched for all the voltage monitoring channels at the same time (via LAUNCH_ABIST bit), or individually (via ABIST_VxMON or ABIST_V1UVLP individual bits).

An individual diagnostic bit is available for each channel once the ABIST is done (ABIST_DONE = 1). The diagnostic flags have no impact on the safety pins. The diagnostic flags must be cleared before launching the next ABIST, using the CLEAR_ABIST bit.

If one of the concerned monitored voltage is out of range (OV or UV), the ABIST on-demand command is ignored. While the ABIST is running, the other monitoring functions are kept available.

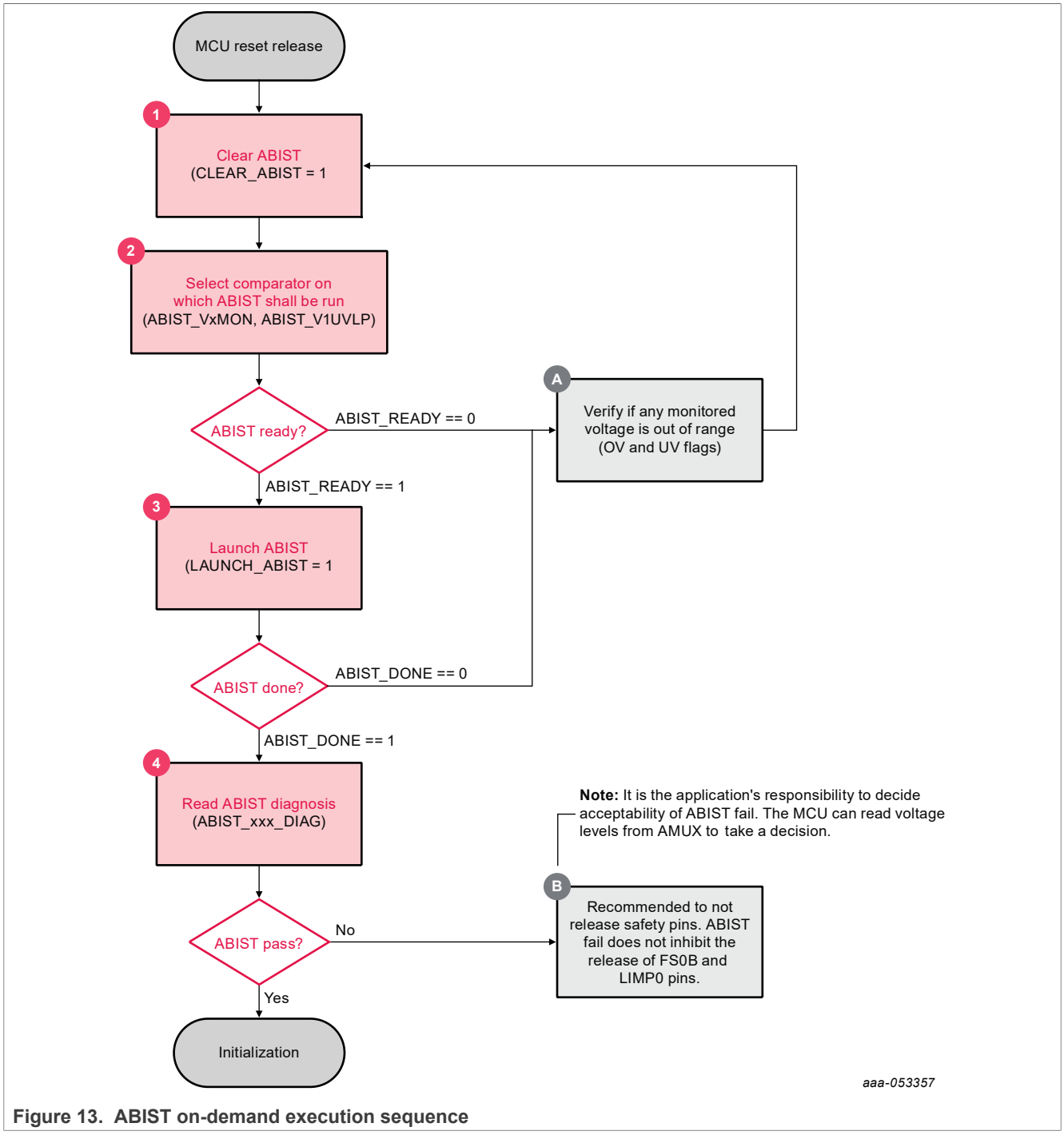

Figure 13. ABIST on-demand execution sequence

4.1.1.3 Protected INIT phase

At power-on reset (POR), the FS23 enters automatically in INIT state. In this mode, the MCU can write the INIT registers (FS_I_xxxxx) configuration of the device safety features and reactions such as watchdog, OV/UV impacts, FCCU and miscellaneous safety behavior.

When the FS23 enters INIT state, LOCK_INIT bit is set to 1, and the cyclic check that protects these registers is disabled. Cyclic redundancy check (CRC) of INIT registers comes in addition to CRC computation during

SPI or I²C transfer and must be computed from INIT registers content. The *FS23 Implementation and Behavior* application note provides information on INIT CRC computation method.

To exit the INIT state, clear the LOCK_INIT bit by writing 1. Then a good watchdog refresh must be sent. The INIT registers, as well as the possibility to select infinite watchdog period configuration, are then protected against write access. The CRC on the INIT registers is activated, and occurs every 5 ms.

The device also enters the INIT state when waking up from LPON or LPOFF states, or when restarting from Fail-safe state (if OTP register loading is not bypassed). This allows the MCU to reconfigure the safety features, if needed.

In Normal mode, the INIT state can be accessed again by sending a GO2INIT request by SPI/I^2C. In this case, if the watchdog is enabled, it must be refreshed every watchdog period.

Note: *If the FS23 goes in LPON or LPOFF or Fail-safe mode while in INIT state, it stays in INIT state, which can lead to misconfiguration of the device. Therefore, it is recommended to read the INIT_S status bit in M_STATUS register before going to LPON or LPOFF mode, and to go only if the device is no longer in INIT state.*

4.1.1.4 Initialization procedure example

An example of FS23 software initialization is given in the *FS23 Implementation and Behavior* application note, with a flowchart and corresponding read and write sequence for SPI or I^2C communication. This example covers launching an ABIST on demand, initialization of INIT registers, watchdog configuration, and exit of initialization phase.

4.1.1.5 Entry to runtime operation

Once the application software has gone through the boot phase, the MCU configures the safety features on both the MCU and the FS23.

Before entering normal operation, the MCU must carry out the following steps in the given order:

1. Configure the FCCU error out state to ‘no fault’.
2. End the INIT state by a successful refresh of the FS23 watchdog.
3. Request the release of the FS0B (and LIMP0 if applicable) output.

When all these actions are completed, the system can enter Runtime mode and execute the application function.

4.1.2 Runtime

All of the following safety mechanisms are active in the SBC and MCU when entering Runtime mode.

4.1.2.1 Watchdog monitoring

The first good watchdog refresh closes the initialization phase (INIT_FS) of the FS23. As soon as the initialization phase is closed, the watchdog monitors the software failures from the MCU by doing a periodical handshake with the FS23 through the SPI communication protocol.

The watchdog is refreshed by the MCU using two keys: 0x5AB2 (default value after POR) and 0xD564. The key is stored in the WD_TOKEN register, and is changed alternatively after each good watchdog refresh. Then, the MCU must write the watchdog answer in the WD_ANSWER register within the expected timing.

The watchdog error counter is incremented when the answer is wrong, not given at the right moment, or not given at all at the end of the watchdog period, as shown in Table 5.

Table 5. Watchdog answer and refresh validation

SPI/I^{2}C	Window watchdog		Timeout watchdog
	CLOSED	OPEN	(always open)
BAD key	WD_NOK	WD_NOK	WD_NOK
GOOD key	WD_NOK	**WD_OK**	**WD_OK**
None (timeout)	N/A	WD_NOK	WD_NOK

4.1.2.2 Fault collection and control unit monitoring

Fault collection and control unit (FCCU) monitoring is part of the safety mechanisms that contribute to reaching ASIL B. FCCU monitoring detects hardware failures from the MCU. It is active as soon as the INIT_FS phase is closed after the first good WD answer. In order to avoid a fault coming from the FCCU, pins must be put in the correct state, or the FCCU should be disabled. FCCU monitoring is deactivated when the device goes to LPON or LPOFF modes.

Multiple configurations are available for FCCU monitoring (by configuration of FCCU_CFG[2:0] bits):

- Activation by pair (bi-stable protocol), typically for S32K3 MCUs, as they embed a fault management unit that only works in bi-stable protocol (default configuration, FCCU_CFG = 001)
- Independent input and/or PWM level on both FCCUx pin
- Single PWM or level input on any FCCUx pin

The independent input modes monitor two different and independent error signals (either steady state or PWM signals). The single-input modes also allow implementation of monitoring from one pin. S32K1 MCUs do not embed a fault management unit, therefore any monitoring mode can be considered.

The fail-safe reaction on RSTB, FS0B, or LIMP0 to an FCCU fault detection is configurable with the FCCUx_[RSTB/FS0B/LIMP0]_IMPACT bits during the INIT phase.

FCCU monitoring by pair (bi-stable protocol)

When connected to the S32K3 MCU FCCU_ERR0 and FCCU_ERR1 pins, the FCCU1 and FCCU2 input pins must be configured by pair to work in bi-stable protocol by default. This configuration cannot be changed because the S32K3 only supports this protocol. The FCCU pins' polarity and the SBC reaction upon a fault can be changed nonetheless.

The default settings for FCCU pins are configured as below:

- FCCU1 = 0 or FCCU2 = 1 is considered as a fault (can be reversed using FCCU12_FLT_POL bits)
- When a fault occurs, the impact can be configured on RSTB, FS0B, and LIMP0 (using FCCU12_[RSTB/FS0B/LIMP0]_IMPACT)

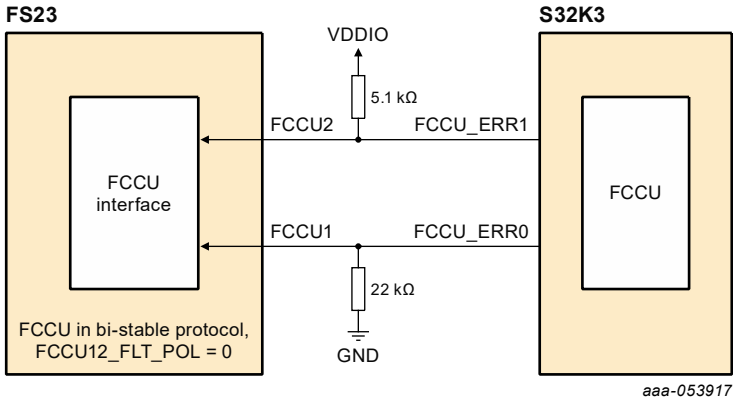

Figure 14. FS23 and S32K3 FCCU connections

Figure 15 shows signal reactions in different phases from the reset to the error phase, and configuration phase for *FCCU1 = 0 or FCCU2 = 1 is a fault* configuration (FCCU12_FLT_POL = 0).

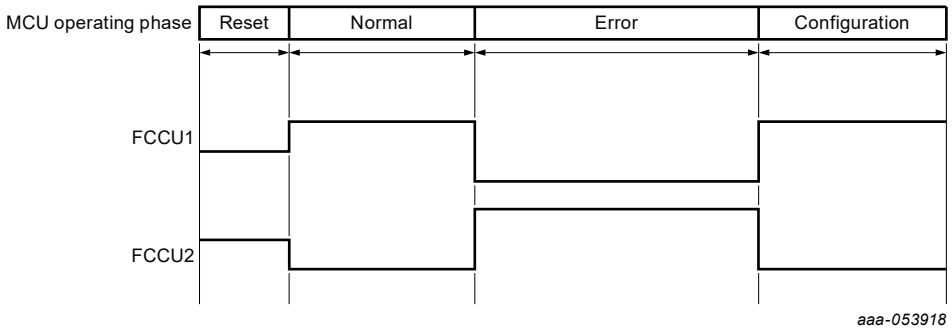

Figure 15. Example of FCCU by pair pins reaction upon a fault

In Runtime mode, it is assumed the S32K3 fail-safe machine (FSM) for the FCCU can be in one of the following two states:

- CONFIG state: Used only to modify the configuration of FCCU from its default setting. This state is only accessible by software during the NORMAL state and can be exited by software or automatically after a WD timeout. The incoming faults, occurring during the configuration phase (CONFIG state), are latched in order to process them when the FCCU transitions to the NORMAL state according to the new configuration.
- NORMAL state: This is the FCCU's operating state when no faults are occurring. It is also the default state on the reset exit.

Figure 16 shows the FCCU state diagram summarizing the different FCCU states and their transitions between one another.

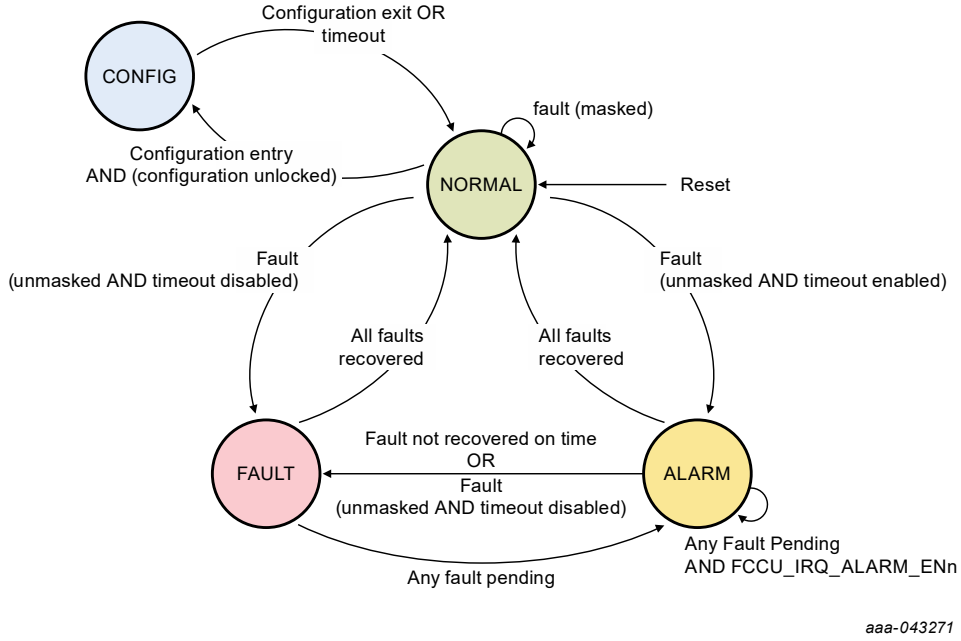

Figure 16. FCCU state machine in S32K3

FCCU independent or single-pin monitoring

When FCCU1 and/or FCCU2 are used independently, the FCCU inputs can monitor two different and independent error signals. These error signals can be either steady state-level signals or PWM signals.

When the error signal is a steady state-level signal, the polarity of each FCCU fault signal is configurable with FCCUx_FLT_POL bits during the INIT phase.

When the error signal is a PWM signal, the error state is reported when the high-level signal duration is inferior to $FCCU12_{HFDET}$ or when the low-level signal duration is superior to $FCCU12_{LFDET}$.

Figure 17 shows a signal example in reset, normal and error phases for the configuration: FCCU_CFG = 111 (FCCU1 input-level monitoring, FCCU2 input PWM monitoring), with FCCU1_FLT_POL = 0 (FCCU1 low level is a fault).

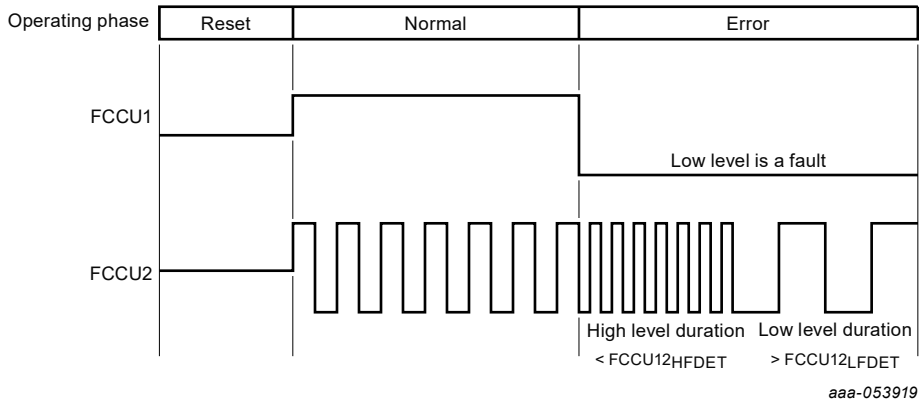

Figure 17. Example of FCCU independent pins reaction upon a fault

4.1.2.3 Reset (RSTB) safety output

The FS23 RSTB pin is meant to be connected to the S32K1/S32K3 bidirectional RESET_b pin. In addition, the RSTB pin is bidirectional, which means the FS23 can assert RSTB to bring the MCU under reset. Also, the MCU can maintain the RSTB asserted externally even if the FS23 is ready to release it.

When entering the Run mode, both reset pins should be high until a reset event happens.

Depending on FS23 OTP configuration, the device transitions into Fail-safe mode when RSTB is stuck low for more than $RSTB_{T8s}$.

4.1.2.4 FS0B and LIMP0 safety outputs

FS0B and LIMP0 safety outputs are meant to bring the whole system into a safe state when enabled, depending on the OTP configuration.

Once the INIT_FS phase is closed after the first good watchdog refresh from the MCU, FS23 safety outputs can only be released once the following conditions are fulfilled:

✓ No fault affecting FS0B reported

✓ Fault error counter = 0

✓ Device in Normal mode

✓ Device not in Debug mode and not in INIT mode

✓ FS_FS0B_LIMP0_REL register filled with a valid release command from the MCU, depending on current WD_TOKEN[15:0] value as per Table 6:

Table 6. FS0B and/or LIMP0 release commands

FS_FS0B_LIMP0_REL[15:0]	B15	B14	B13	B12	B11	B10	B9	B8	B7	B6	B5	B4	B3	B2	B1	B0
Release FS0B	0	1	1	NOT(WD_TOKEN[0:12])												
Release LIMP0	1	1	0	NOT(WD_TOKEN[3:15])												
Release both FS0B and LIMP0	1	0	1	NOT(WD_TOKEN[0:6])							NOT(WD_TOKEN[10:15])					

The step-by-step procedure to release FS0B and LIMP0 is described below:

1. Send WD_ERR_LIMIT × FLT_ERR_CNT + 1 good watchdog refreshes to clear the fault error counter. Each time the watchdog refresh counter (WD_RFR_CNT) is maxed out, FLT_ERR_CNT is decremented by 1.
2. Read the FS_WD_TOKEN value.
3. Swap and/or reverse the bits of this value, depending on the desired command.
4. Write bits from 12 to 0 obtained from previous step into FS_FS0B_LIMP0_REL register. Bits 15 to 13 are used to select which safety output will be released.

Once this procedure is completed, FS0B and/or LIMP0 are released to a high logic level, safety mechanisms are enabled, and the system can now enter the Runtime mode.

4.1.2.5 Optional disabling of watchdog and FCCU

In the FS23 device, the watchdog and FCCU functions can be disabled during the INIT sequence. This is recommended during development and debug of the application.

Disabling of watchdog monitoring

On the FS23, when enabled by OTP, the watchdog can only be disabled during the initialization phase via SPI or I^2C commands:

- To disable the watchdog window, the watchdog window period configuration bits WDW_PERIOD[3:0] of the FS_WDW_CFG register must be set to 4b'0000.
- To disable the watchdog window with FCCU error and recovery strategy enabled, the watchdog window period configuration bits WDW_RECOVERY[3:0] of the FS_WDW_CFG register must be set to 4b'0000.

The watchdog disable is effective when the INIT phase is closed.

Disabling of FCCU monitoring

The FCCU input pins can be configured by pair, or single independent inputs using FCCU_CFG[2:0] bits. The FCCU monitoring is active as soon as the INIT phase is closed. Pins must be put in the correct state at this point in order to avoid a fault coming from the FCCU monitoring, or FCCU should be disabled.

FCCU monitoring can be disabled with the FCCU_CFG[2:0] bits of the FS_I_FCCU_CFG register, by setting FCCU_CFG[2:0] to 4b'000.

FCCU monitoring is deactivated when the device goes to LPON or LPOFF modes.

4.1.3 Standby mode

In Standby mode, only a portion of the S32K3 is powered, so only some rails must be supplied. The Very Low Power Run (VLPR) mode is the equivalent mode for S32K1 devices. When the MCU is in Standby mode, it performs no safety-related functions.

The Standby mode corresponds to LPON mode for the FS23 device. In this mode, only the necessary regulators are kept on: V1 regulator is always on in LPON, while V2 and V3 are off by default. Though, V2 and V3 can be configured to stay on in LPON.

If Standby mode is considered safety-related for the MCU by the application, then system-level checks must be implemented to ensure the desired safety level. This mode is assumed to be a safe state with no critical activity in SBC, therefore FS0B pin is asserted. Before moving to Standby mode, the FCCU error out signals must be asserted by software to transition the system to a safe state. The MCU's FCCU_ERR0 must be asserted active low during standby and FCCU_ERR1 must be asserted active high during standby.

The VLPR entry and exit for S32K1 is covered in section "System Mode Controller" of S32K1 reference manual.

The Standby mode entry and exit sequences for S32K3 are covered in section "Mode Entry Module" of S32K3 reference manual.

The SBC can wake up from LPON through any of the following wake-up mechanisms, which can be configured through SPI or I^2C:

- WAKE1, WAKE2, HVIOx and LVIOx pins
- Long duration timer (LDT) expiration
- CAN and LIN via wake-up pattern
- GO2NORMAL SPI or I^2C command via M_SYS_CFG

4.1.4 Safe state

According to ISO 26262[1], a safe state is an "operating mode, in case of a failure, of an item without an unreasonable level of risk".

The S32K1/S32K3 is in a safe state when it is unpowered or is indicating a fault externally and/or in reset. While the MCU is indicating a fault on its error out (S32K3 only) or reset pins, the FS23 must be configured to provide a safe state transition signal to ensure the system is in a safe state in the presence of a fault in the MCU.

The FS23 is an ASIL B device with a safe state ensured by a fail-safe state in the main state machine (no fail-safe sate machine).

4.1.4.1 Fault impact configuration

The FS23 has three safety outputs: RSTB, FS0B, and LIMP0. These safety output pins are used to guarantee the system safe state. All these safety outputs are active low. The assertion of the safety outputs depends on the device configuration during the initialization phase. RSTB and FS0B are activated during power up and can only be released when the device is in Normal mode. LIMP0, on the contrary, will be released at startup and will only be asserted when a fault occurs.

Some faults can be configured to assert (or not) RSTB, FS0B, and/or LIMP0, while some other faults assert safety pins without the possibility of being configured. For the complete list of configurable and non-configurable faults, refer to "Fault source and reaction" in the FS23 data sheet.

4.1.4.2 Safe state entry due to fault in FS23 or S32K

- The FS23 uses its fault error counter to bring the system into Safe state when a fault related to FS23 itself occurs or when the fault is caused by external events. When the fault error counter reaches its maximum value, the system transitions into Fail-safe (FS) state.
- Fault in MCU indicated by FCCU error indication outputs: The fault recovery strategy feature is enabled by SPI/I^2C using WDW_REC_EN bit. This function extends the watchdog window to allow the MCU to perform a fault recovery strategy. The goal is to not reset the MCU while it is trying to recover the application after a failure event. When a fault is triggered by the MCU via its FCCU pins, the FS0B and LIMP0 pins are asserted by the device depending on the FCCU error impact configuration, but not RSTB, and the watchdog window duration becomes automatically an open window (no more duty cycle). This open window duration is configurable with the WDW_RECOVERY[3:0] bits.
- The transition from WDW_PERIOD to WDW_RECOVERY happens when the FCCU pin indicates an error and FS0B or LIMP0 is asserted. If the MCU sends a good watchdog refresh before the end of the WDW_RECOVERY duration, the device switches back to the WDW_PERIOD duration and associated duty cycle if the FCCU pins does not indicate an error anymore. Otherwise, a new WDW_RECOVERY period is started. If the MCU does not send a good watchdog refresh before the end of the WDW_RECOVERY duration, then a reset pulse is generated, and the device goes to Fail-safe state.

1 International Standard ISO 26262-1, Road vehicles - Functional Safety, Part 1: Vocabulary

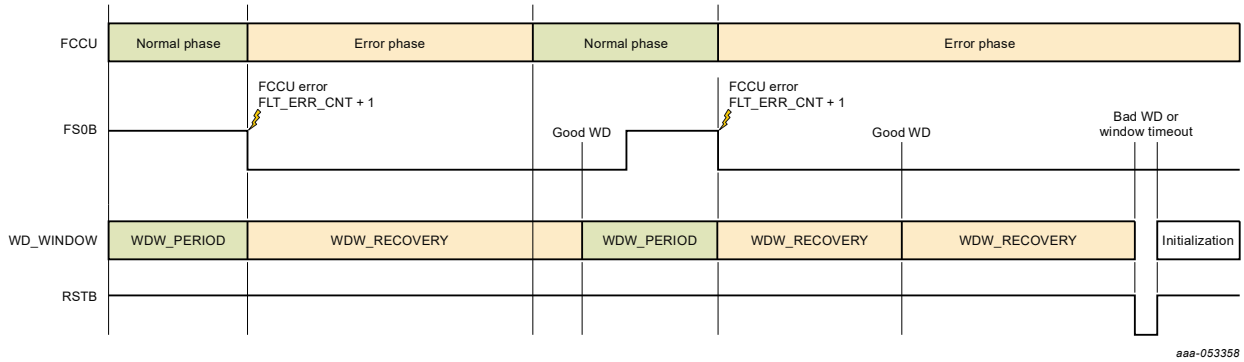

Figure 18. Fault recovery strategy principle

- Fault indicated by inability to refresh the watchdog: The FS23 has a watchdog error counter to bring the system into Safe state when an incorrect watchdog refresh occurs. When the watchdog error counter reaches its maximum value, the fail-safe reaction is imposed on safety output(s). The watchdog refresh counter is used to decrement the fault error counter when the watchdog is continuously being serviced (maximum value is configurable) by the MCU, indicating its correct operation.

4.1.5 System safe state

The system safe state is ensured by safety output pins RSTB, FS0B, and LIMP0. All of those safety outputs are active low. RSTB and FS0B are activated during power up and can only be released when the device is in Normal mode. LIMP0, on the contrary, will be released at startup and will only be asserted when a fault occurs. The three pins are managed independently in parallel of the main state machine.

Figure 19 gives and overview of the safety features implemented in the FS23 and their connection to the system safe state.

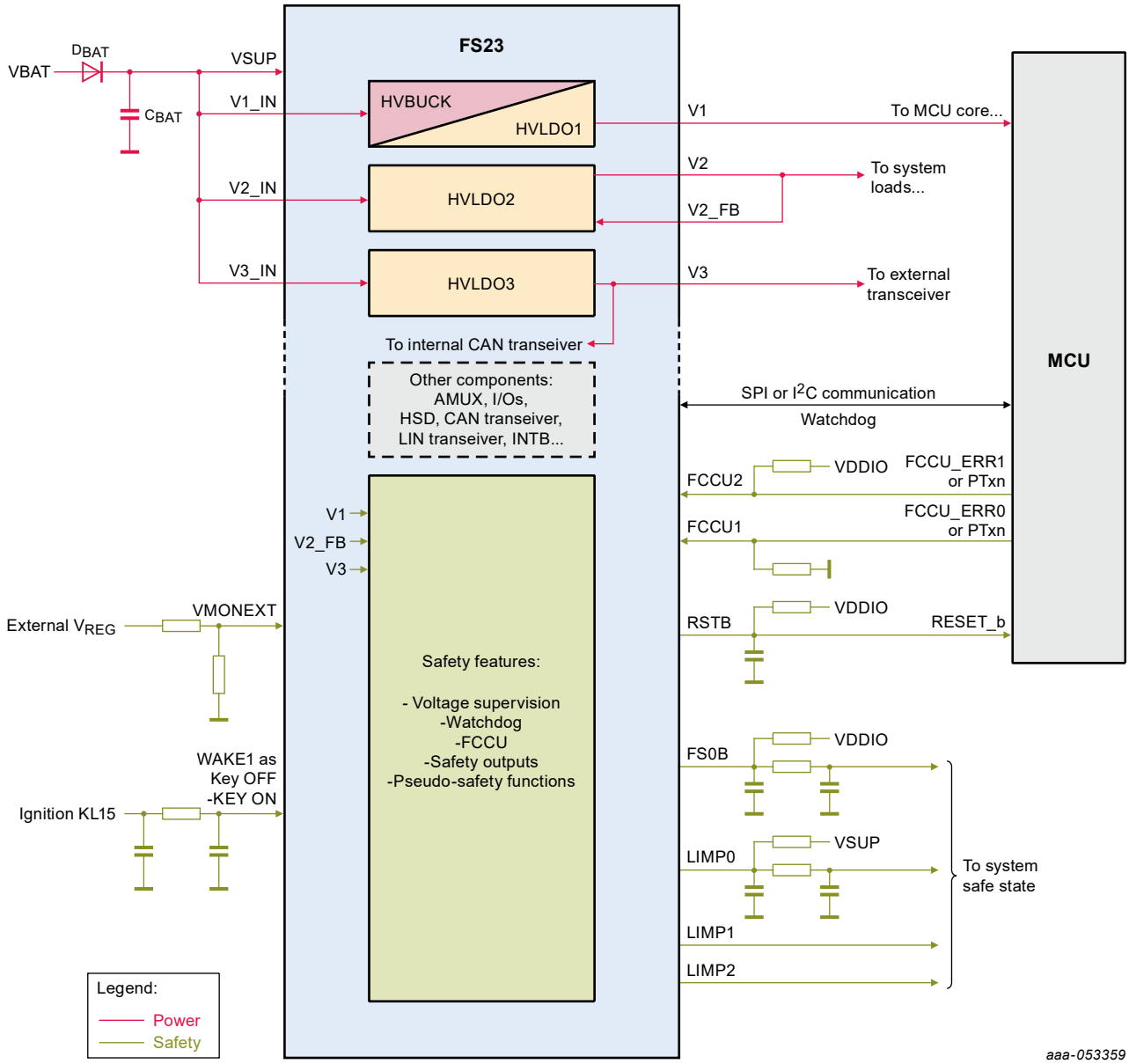

Figure 19. FS23 safety features and system safe state

Safety pins and modes

In Fail-safe state and LPOFF mode, all safety pins are asserted to ensure system safe state.

LPON mode is assumed to be a safe state with no critical activity, and FS0B is asserted low.

In normal operation when all safety pins are released, the fault error counter is incremented each time a fault is detected by the FS23. Critical fault sources have a mandatory action on safety pins, and other fault sources can be configured to assert safety pins depending on desired behavior of the system. In the FS23 data sheet, “Application related Fail-Safe fault list and reaction” lists all the faults and their impact on RSTB, FS0B, and LIMP0 pins with regard to the device configuration by OTP and/or by I^2C/SPI.

LIMP1 and LIMP2 pseudo-safety functions

Two pseudo-safety outputs LIMP1 and LIMP2 can be used when configuring general purpose I/Os as LIMP1 or LIMP2 functions. LIMP1 and LIMP2 functions are following LIMP0 assertion and release. Therefore, these pseudo-safety functions provide access to two extra output pins for system safe state.

LIMPx_CFG[1:0] bit allows the user to choose LIMP1 and LIMP2 functions behavior as:

- asserted to a static level (high or low),
- asserted as PWM (configurable polarity).

Table 7 shows the available behaviors for LIMP1 pseudo-safety function when asserted. When configured as PWM, LIMP1 is static when no fault is reported.

Table 7. LIMP1 pseudo-safety function available behaviors when asserted

LIMP1_CFG[1:0]	Behavior when LIMP0 released	Behavior when LIMP0 asserted
00	Default high	f_{PWM} = 1.25 Hz with 50 % duty cycle
01	Default high	Active low
10	Default low	f_{PWM} = 1.25 Hz with 50 % duty cycle
11	Default low	Active high

Table 8 shows the available behaviors for LIMP2 pseudo-safety function when asserted. When configured as PWM, LIMP2 is static when no fault is reported, and toggles at 100 Hz when asserted. Its duty cycle is configurable using LIMP2_DC_CFG[1:0] bit.

Table 8. LIMP2 pseudo-safety function available behaviors when asserted

	Behavior when LIMP0 released	Behavior when LIMP0 asserted			
LIMP2_CFG[1:0]	*LIMP2_DC_CFG[1:0]*	*00*	*01*	*10*	*11*
00	Default high	f_{PWM} = 100 Hz with 20 % DC	f_{PWM} = 100 Hz with 10 % DC	f_{PWM} = 100 Hz with 5 % DC	f_{PWM} = 100 Hz with 2.5 % DC
01	Default high	Active low			
10	Default low	f_{PWM} = 100 Hz with 20 % DC	f_{PWM} = 100 Hz with 10 % DC	f_{PWM} = 100 Hz with 5 % DC	f_{PWM} = 100 Hz with 2.5 % DC
11	Default low	Active high			

4.2 Fault recovery process

The fault recovery process is fully supported by S32K3 + FS23 devices (fault management unit is not present on S32K1 series). This strategy is useful to expand the availability of the application when a fault occurs on a hardware item of the S32K3. This means that S32K3 and FS23 can allow the software to recover within the application's fault tolerant time interval (FTTI), instead of preventing the application from running as soon as a hardware error is detected on the MCU side.

4.2.1 Configuration on FS23

On the FS23, two fields are specific to the fault recovery process configuration in the FS_WDW_CFG register:

- WDW_REC_EN bit: to enable the feature.
- WDW_RECOVERY[3:0] bits: to configure the recovery open window duration, between 1 ms and 1024 ms.

4.2.2 List of fault sources in S32K3

As a reminder, the following list depicts all internal faults that can be detected and signaled with FCCU pins.

Table 9. Internal faults list

Channel #	Source module	Description	Recommended recovery mechanism
NCF[0]	M7 LS and Core LOCKUP; HSE LOCKUP	Lockup	Functional reset
NCF[1]	Interconnect: All EDC bus gaskets; XBIC monitors, and platform gaskets	Gasket error or main XBAR	Functional reset
NCF[2]	ECCerrors: PRAMC; TCMs; Caches; eDMA; EDC after ECC (PRAMC); HSE RAM errors	All SRAM ECC uncorrectable error ERM_ SRAMor ECC cache memory error ERM_ M7_Dcache + Icache ECC or read done by safety masters DMA or FMU: Coming from flash. Newly added or HSE RAM ECC	Functional reset
NCF[3]	All flash errors: FMU; PFALSH; DCM flash	Flash ECC uncorrectable error (design path FMU - PFlashC- ERM- FCCU) or FMU: Coming from flash or Error state to FCCU from DCM	Functional reset
NCF[4]	Voltagerelated errors: PMC 1.1 V and 2.5 V GnG; PAD overvoltage	1.1 V or 2.5 V detector	Interrupt followed by SBC initiated POR recovery initiated in interrupt service routine
NCF[5]	Debug and test monitoring	Monitoring of debug activation or accidental partialtest mode activation (to be defined by DFT team)	Interrupt
NCF[6]	INTM	INTM error	Interrupt followed by a reset on the second fault
NCF[7]	SW notification	Software notification	Interrupt

For the first four NCFs, NCF[0] to NCF[3], the recommended recovery mechanism is a functional reset. In which case, the error out EOUT[1:0] signals are generated to report the event to the FS23 SBC. EOUT[1:0] signals are respectively bounded to FCCU_ERR[1:0] pin functions.

Multiple use cases of faults detected by the FCCU are presented in the following sections to illustrate signal generation with applicative scenarios.

4.2.3 Use case 1: Alarm interrupt, SW recovers (local recovery)

In use case 1, a fault has been reported to the FCCU of the S32K3. As soon as the fault is reported, the software can recover from the fault and FCCU_ERR[1:0] pins are not asserted by the S32K3. As a result, the FS23 does not detect an error through its FCCU1 and FCCU2 pins and does not react. Figure 20 is a timing diagram illustrating this local recovery scenario.

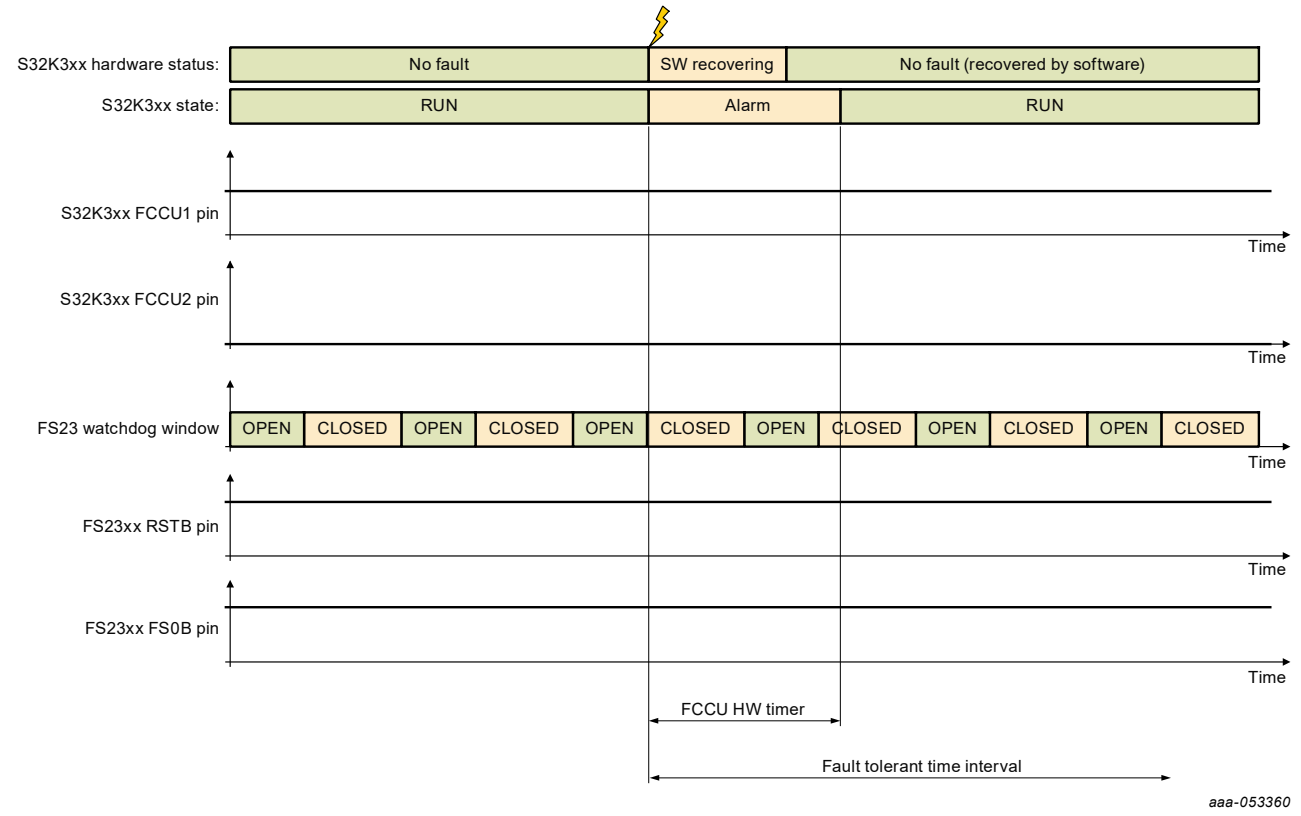

Figure 20. Local recovery timing diagram

With this approach, the application can continue to run without any interruption and the fault is recovered. The S32K3 alarm must take care of the FCCU HW timer, FS23 watchdog window, and FTTI.

4.2.4 Use case 2: Alarm interrupt with escalation, SW does not recover (global recovery)

In use case 2, a fault has been reported to the FCCU of the S32K3. As soon as the fault is reported, the software tries to recover from the fault before the FCCU HW timer expires without success. Therefore, the S32K3 enters its error state and asserts the FCCU_ERR[1:0] pins. As a result, the FS23 detects an error through its FCCU1 and FCCU2 pins and enlarges the open window to allow time for the MCU to perform a good watchdog refresh. From here, the scenario can be divided in two:

- **Case A:** The MCU successfully recovers and can send a good watchdog refresh to the FS23 within the new open window timing. In this case, the FS23 will not assert its safety outputs and the application is still available. Figure 21 shows this scenario, where the application can continue to run without any interruption and the fault is recovered.

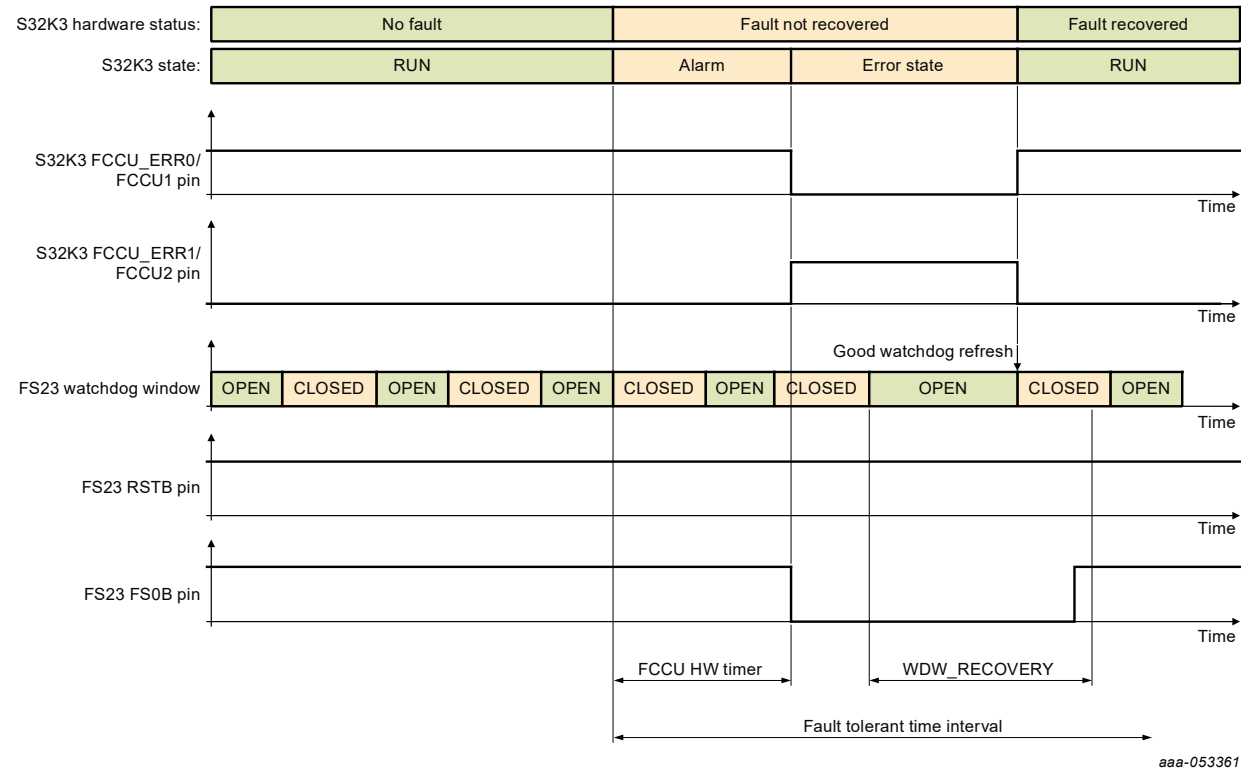

Figure 21. Successful global recovery timing diagram

- **Case B:** The MCU is still not able to send a good watchdog refresh to the FS23 within the new open window timing. In this case, the FS23 asserts its safety outputs to go to application safe state. Figure 22 illustrates this scenario where the application transitions into the safe state because the MCU was not able to send a good watchdog refresh key within the extended open window.

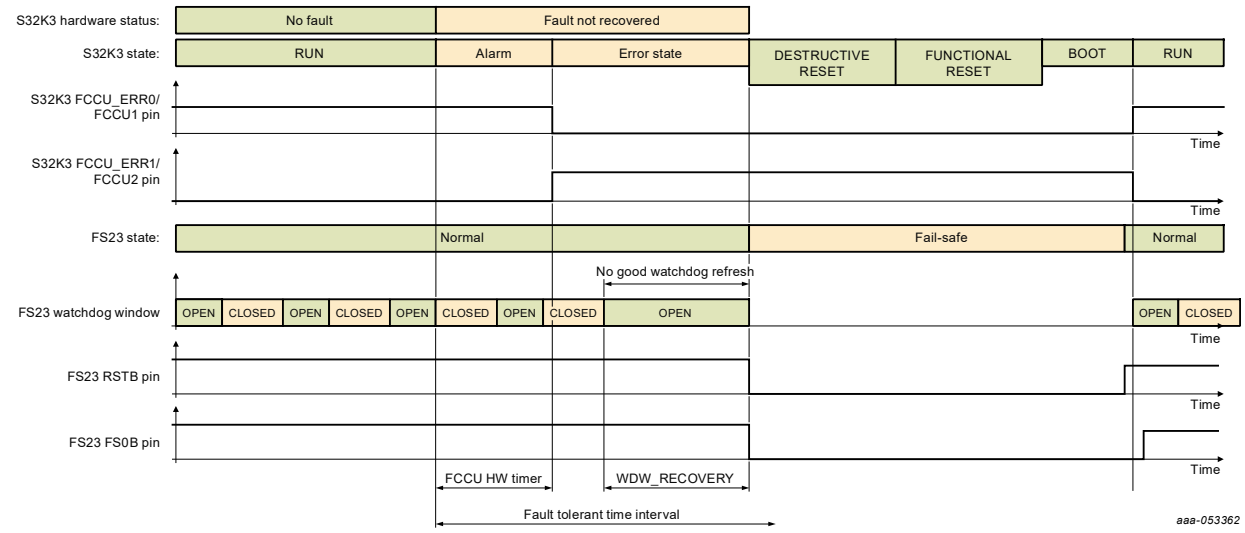

Figure 22. Unsuccessful global recovery timing diagram

4.2.5 Use case 3: Fault recovery feature disabled

In use case 3, the fault recovery feature is disabled, therefore the application must transition to a safe state as soon as an MCU error occurs. To support this, the FS23 must be properly configured with the fault recovery disabled.

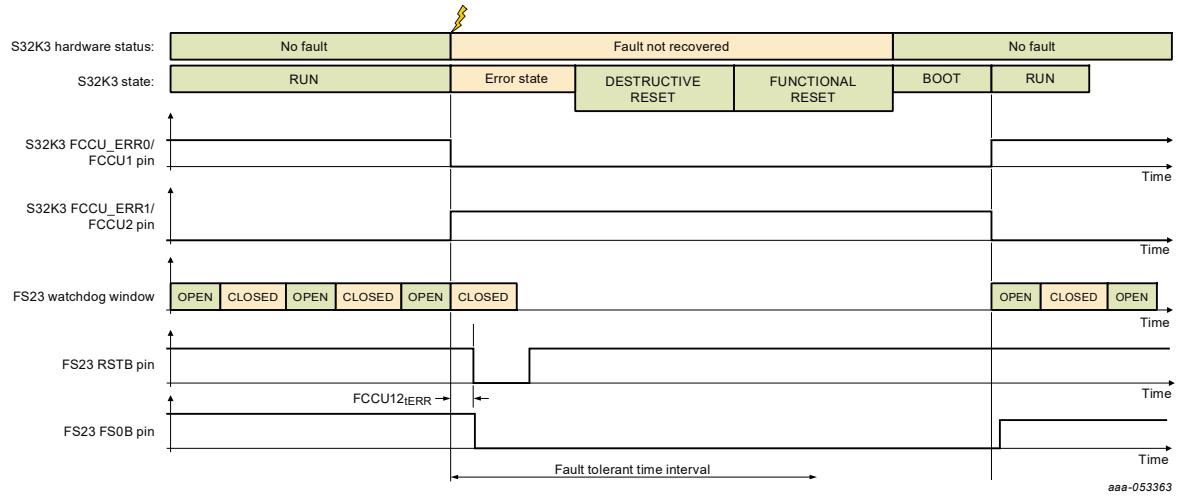

Figure 23. Fault recovery feature disabled

Note: *The FCCU12$_{tERR}$ is described in the FS23 data sheet.*

4.3 Software enablement

NXP's FS23 SBC and S32K1/3 microcontrollers offer a hardware and software solution to fulfill functional safety requirements at application level. The software elements are intended to help the customer implement the hardware elements' features in safety-related applications.

4.3.1 AUTOSAR software drivers

Low-level software driver components are provided as part of the basic enablement for the device, and thus do not incur an extra charge:

- FS23 AUTOSAR software drivers: AUTOSAR and ISO 26262-compliant basic startup drivers for low-level interfaces. Technical documentation is available as part of the software driver package, detailing supported features, such as:
  - SPI access register function and events handling (SBC_FS23);
  - CAN/LIN function (CANTRCV_FS23 and LINTRCV_FS23);
  - Watchdog function (WDG_FS23);
- S32K1 software resources: Real-time drivers (RTD) for S32K1, reference software and more.
- S32K3 software resources: RTD for S32K3, reference software and more.

RTDs are a set of drivers supporting real-time software on AUTOSAR and non-AUTOSAR applications targeting ISO 26262 compliance for all software layers. General information on these standard and low-level drivers is also available on the Real-Time Drivers (RTD) webpage.

5 Abbreviations

Table 10. Abbreviations

Acronym	Description
ABIST	Analog built-in self-test
CRC	Cyclic redundancy check
FCCU	Fault collection and control unit
FS	Fail-safe
HS	High side
LPON	Low-power ON, also known as Standby mode
LPOFF	Low-power OFF
OTP	One-time programmable
SBC	System basis chip

6 References and helpful links

Documentation

1. AN14128 - FS23 hardware guideline, application note
2. AN14129 - FS23 implementation and behavior, application note
3. FS23 data sheet
4. FS23 safety manual (use the secure files button and log in)
5. S32K1 data sheet
6. S32K1 reference manual
7. AN5426 - Hardware design guidelines for S32K1, application note
8. S32K3 data sheet
9. S32K3 reference manual

Software resources

1. FS23 AUTOSAR software drivers
2. S32K1 software resources
3. S32K3 software resources
4. Real-Time Drivers (RTD) general information

Evaluation resources

1. FS23 graphical user interface (GUI)
2. FS23 programming board
3. FS23 evaluation board for HVBUCK variant
4. FS23 evaluation board for LDO variant

7 Revision history

Table 11. Revision history

Document ID	Release date	Description
AN14068 v. 2.0	21 November 2024	• Changed security status from confidential to public • Global: corrected links • Updated legal information
AN14068 v. 1	12 January 2024	Initial version

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

Suitability for use in automotive applications (functional safety) — This NXP product has been qualified for use in automotive applications. It has been developed in accordance with ISO 26262, and has been ASIL classified accordingly. If this product is used by customer in the development of, or for incorporation into, products or services (a) used in safety critical applications or (b) in which failure could lead to death, personal injury, or severe physical or environmental damage (such products and services hereinafter referred to as "Critical Applications"), then customer makes the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. As such, customer assumes all risk related to use of any products in Critical Applications and NXP and its suppliers shall not be liable for any such use by customer. Accordingly, customer will indemnify and hold NXP harmless from any claims, liabilities, damages and associated costs and expenses (including attorneys' fees) that NXP may incur related to customer's incorporation of any product in a Critical Application.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Figures

Contents